

09/937410

TECHNICAL DRAWING

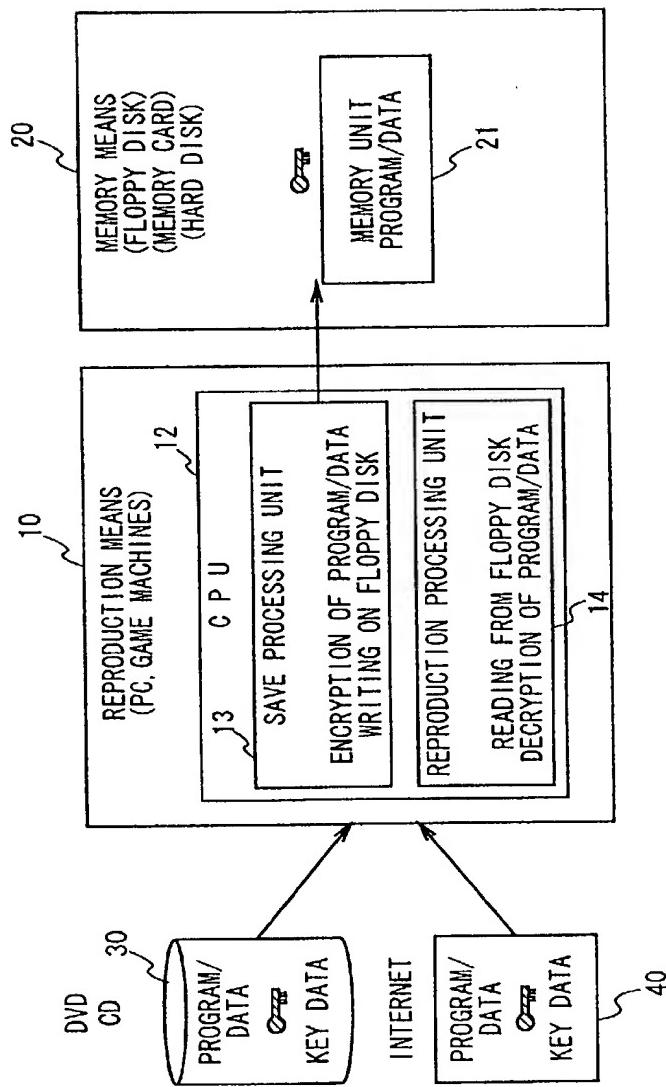
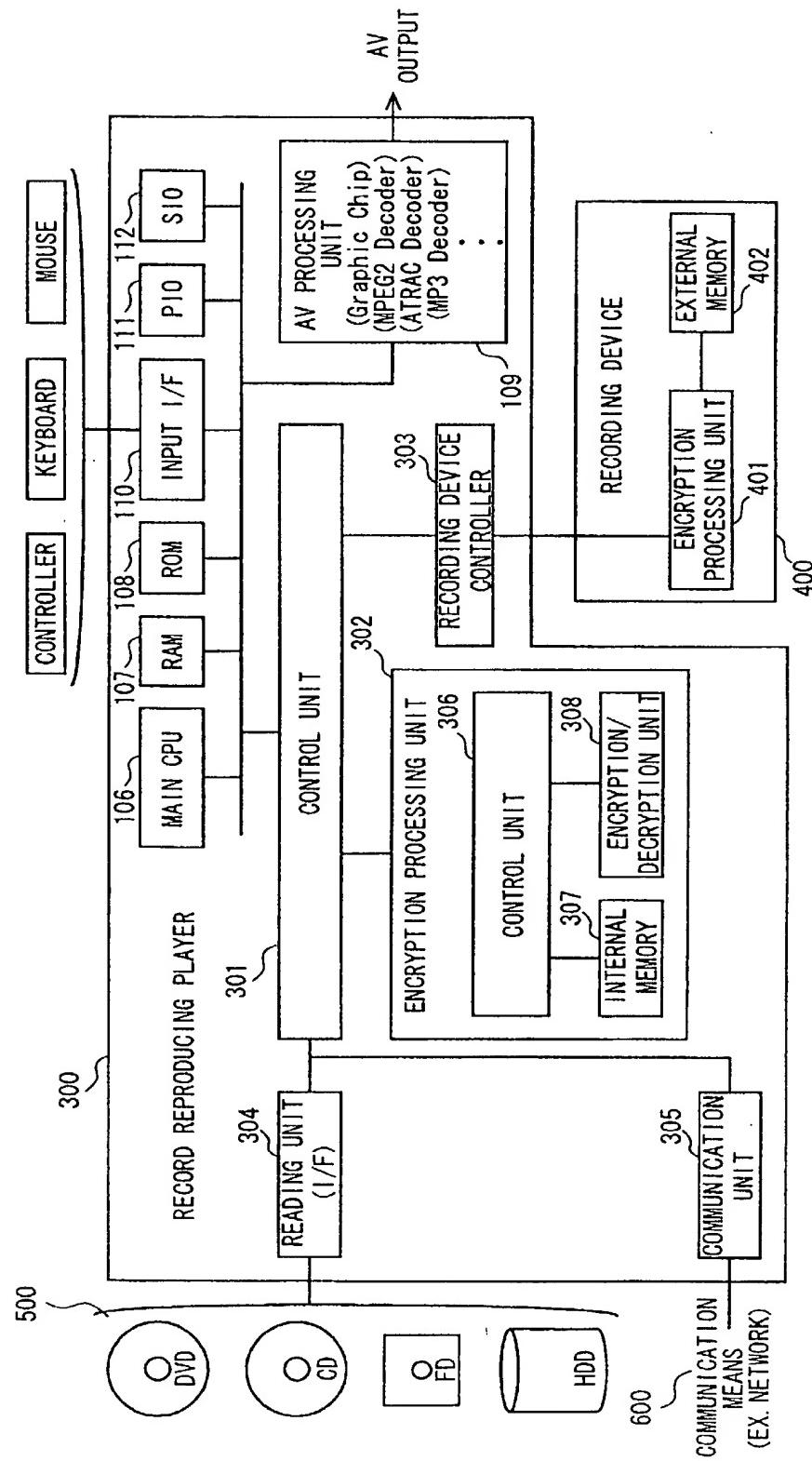


FIG. 1



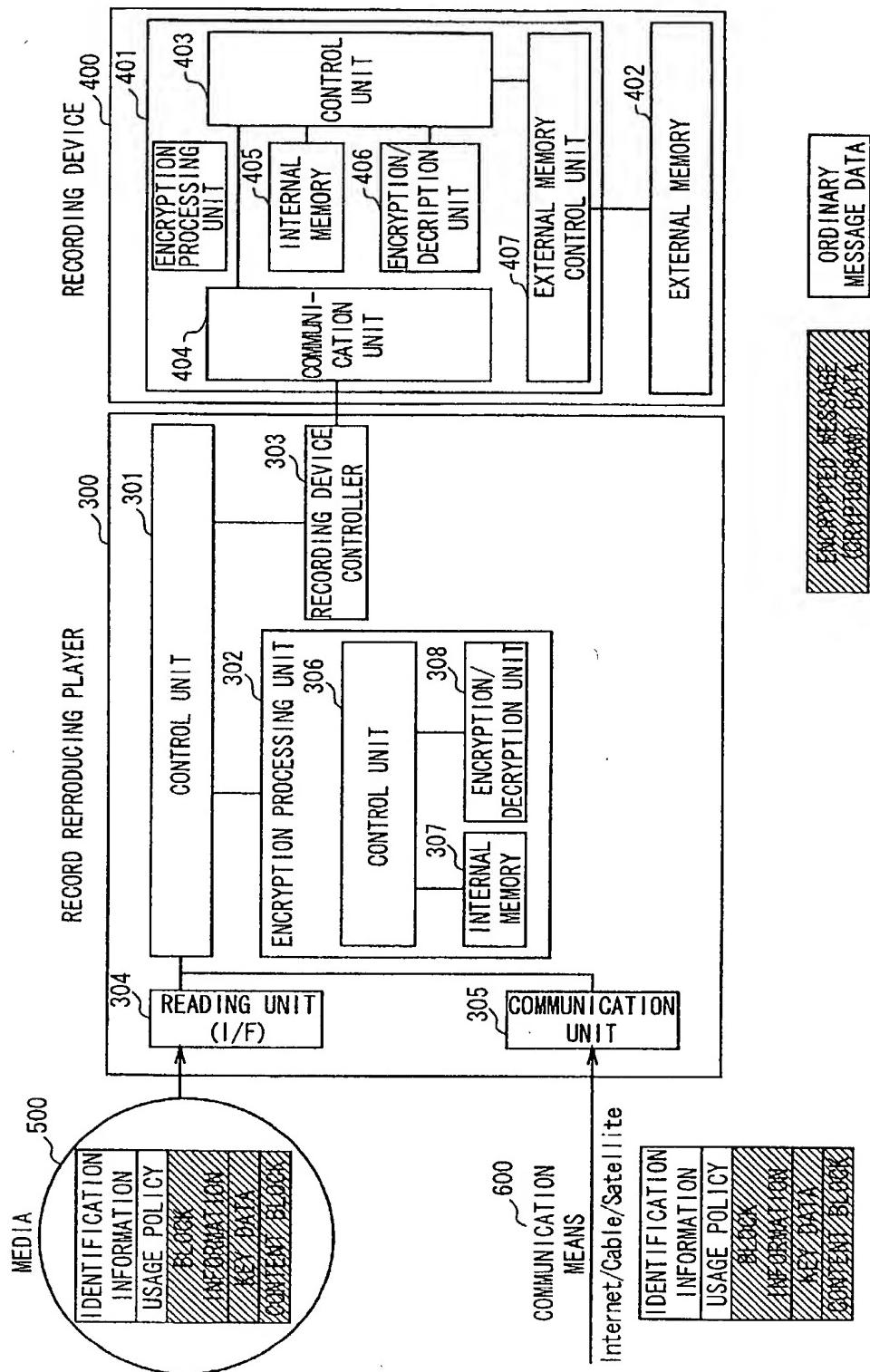
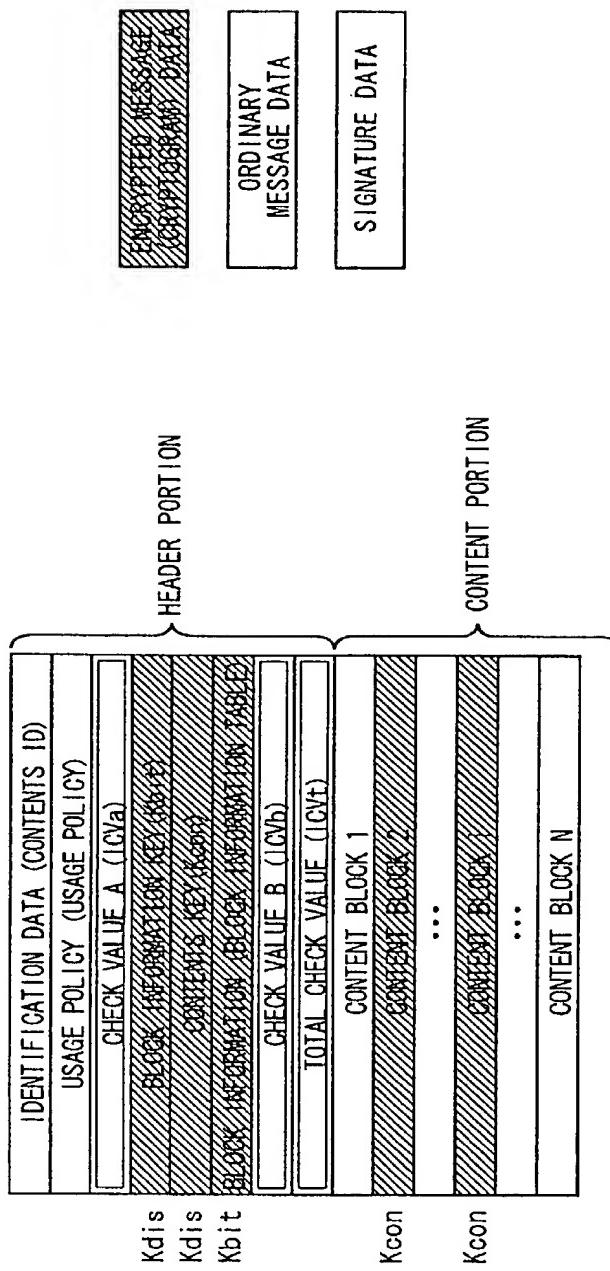


FIG. 3

TOC/T - DIFFERENCE

09/937410



DATA FORMAT ON MEDIA & COMMUNICATIONS ROUTE

FIG. 4

09/937410

TOP SECRET // DIPLOMATIC

HEADER LENGTH
CONTENT LENGTH
FORMAT VERSION
FORMAT TYPE
CONTENT TYPE
OPERATION PRIORITY
LOCALIZATION FIELD
COPY PERMISSION
MOVE PERMISSION
ENCRYPTION ALGORITHM
ENCRYPTION MODE
INTEGRITY CHECK METHOD

USAGE POLICY

FIG. 5

09/937470

Kbit

BLOCK NUMBER	
BLOCK	BLOCK LENGTH
1	ENCRYPTION FLAG
	ICV FLAG
	ICV1
.	
.	
.	
BLOCK	BLOCK LENGTH
N	ENCRYPTION FLAG
	ICV FLAG
	ICVN

BLOCK INFORMATION

FIG. 6

09/937410

"DEFFEE" ORIGIN: E600

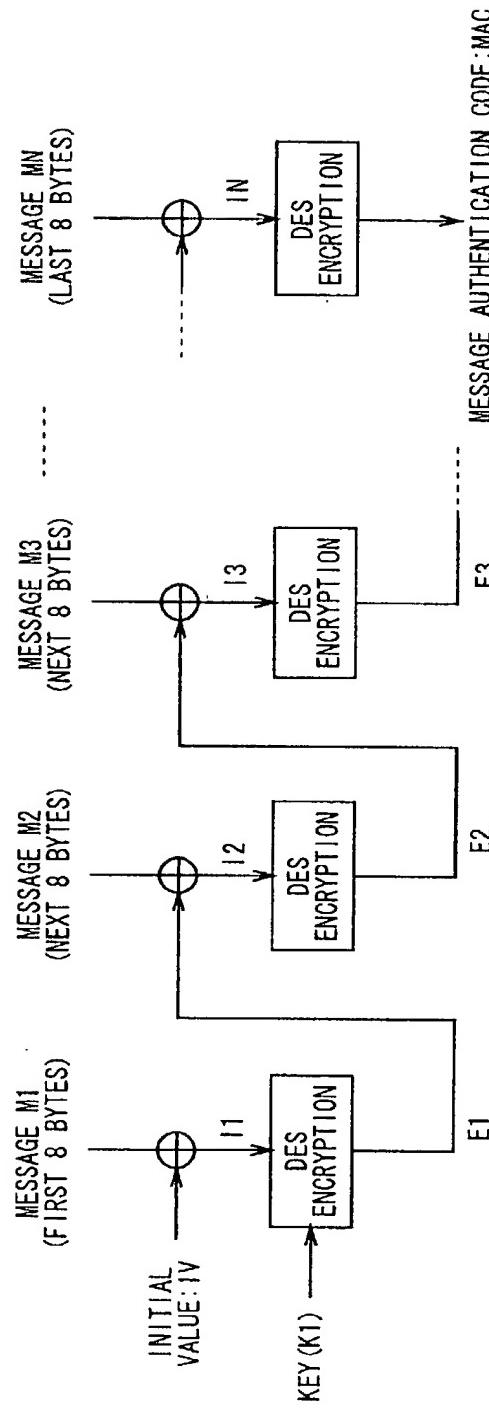


FIG. 7

09/937410

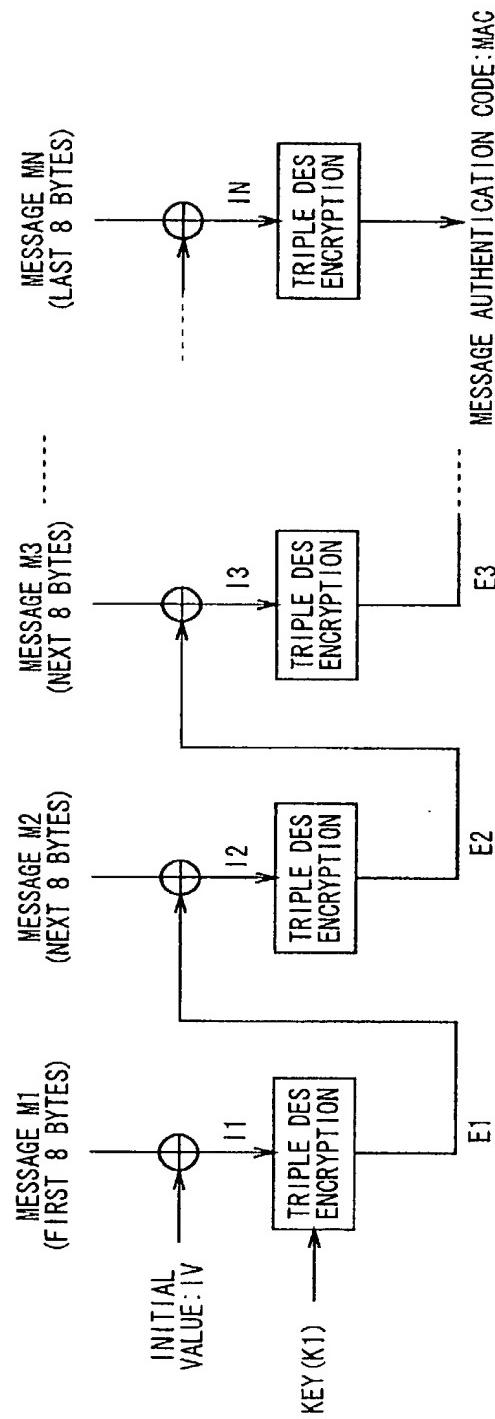


FIG. 8

09/937410

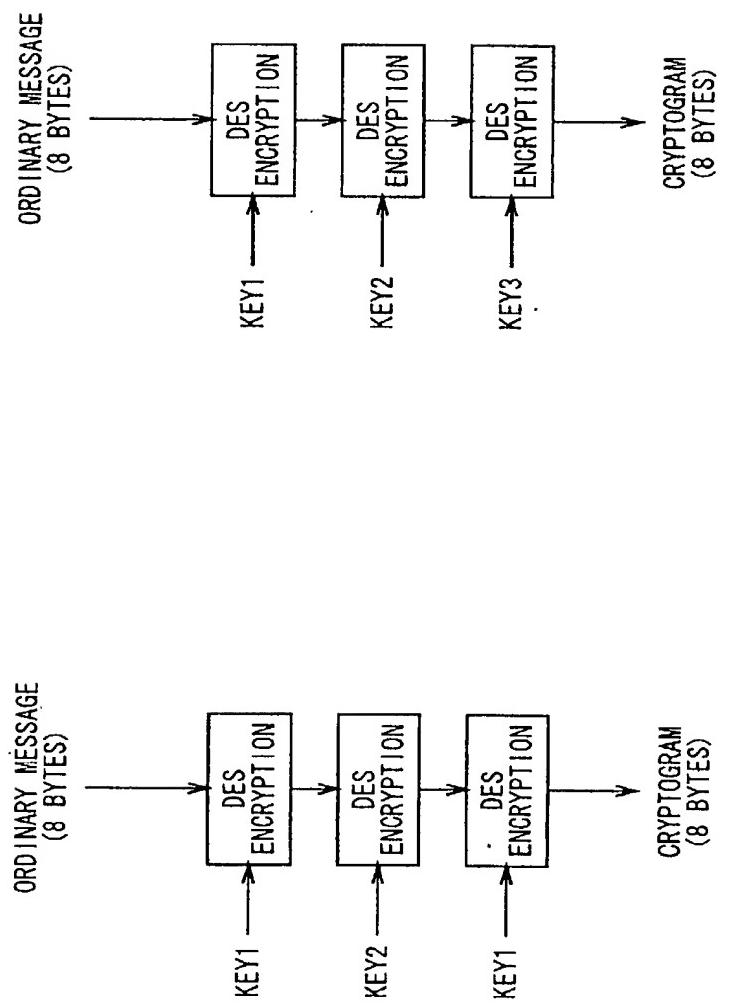


FIG. 9

(A)

(B)

09/937410

TOP SECRET // ODT//~~REF ID: A660~~

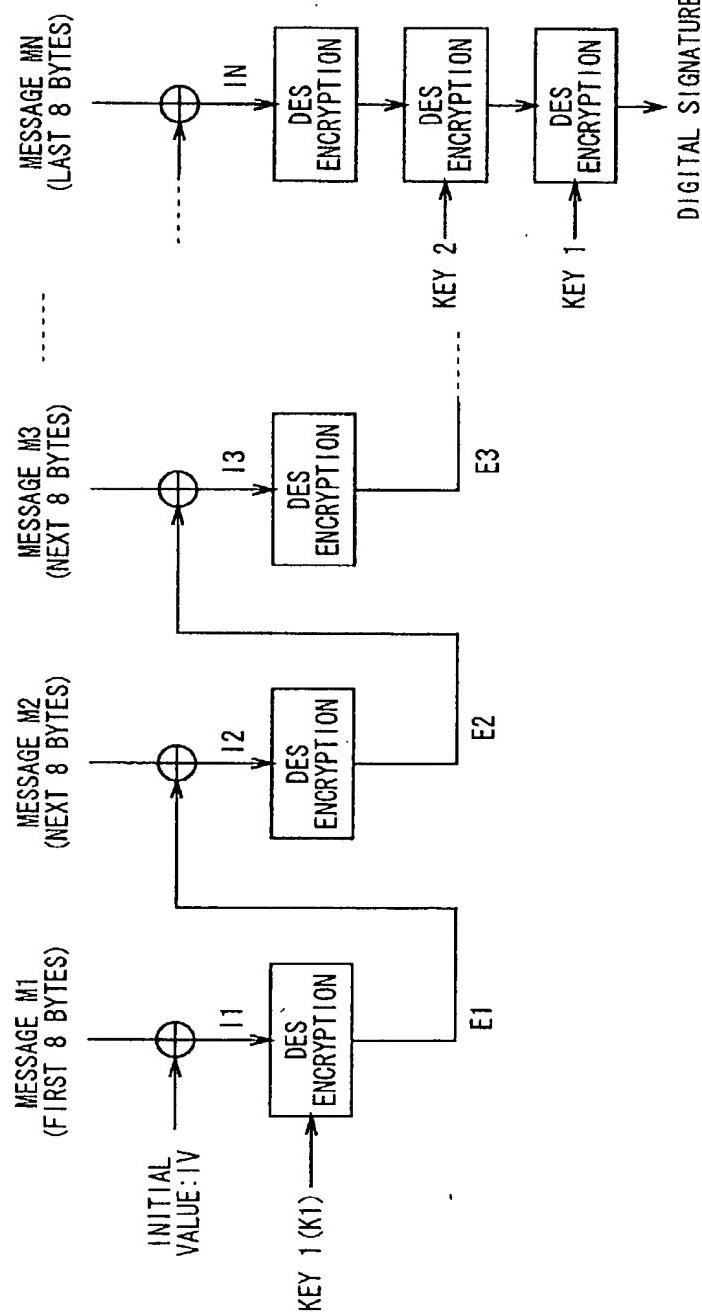


FIG. 10

TOP SECRET - OTTAWA 650

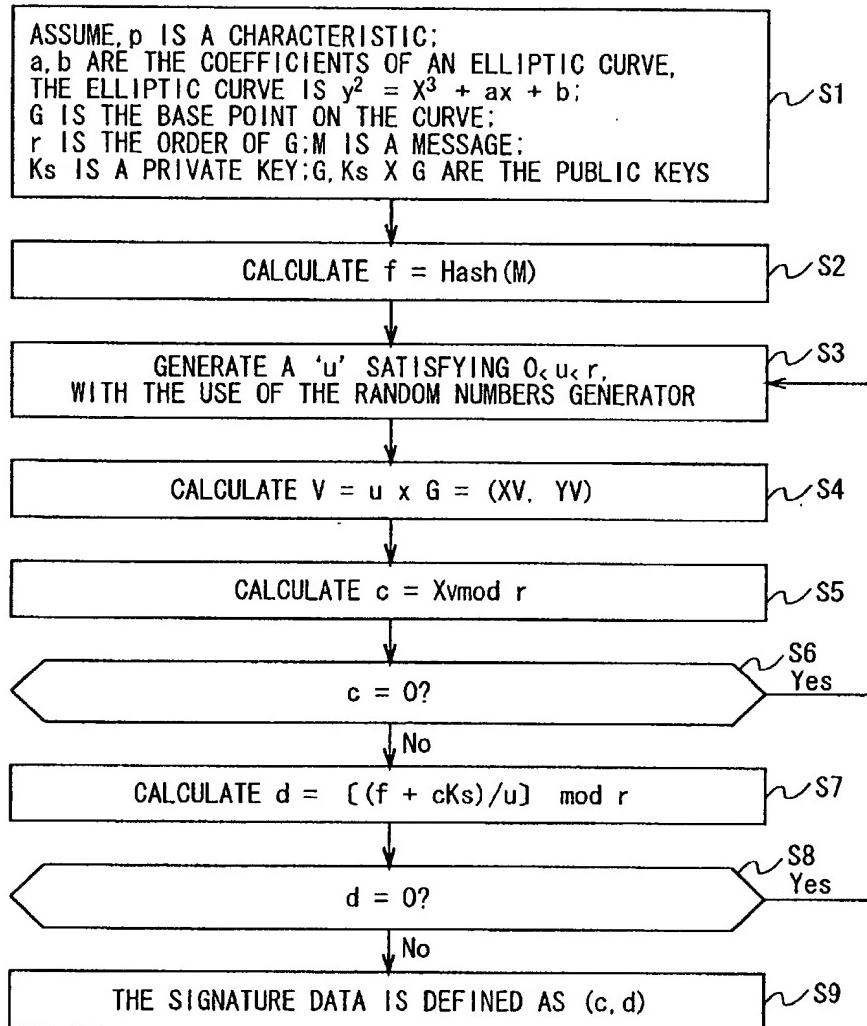
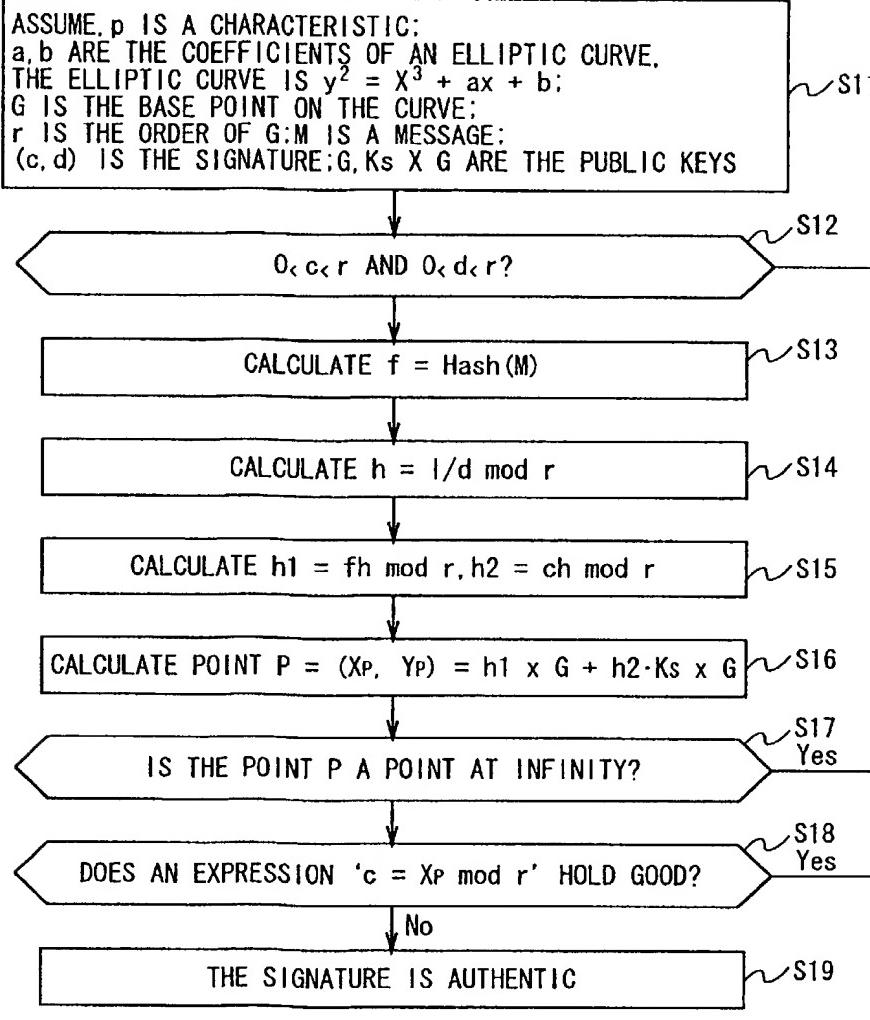
GENERATION OF SIGNATUREGENERATION OF SIGNATURE (IEEE P1363/D3)

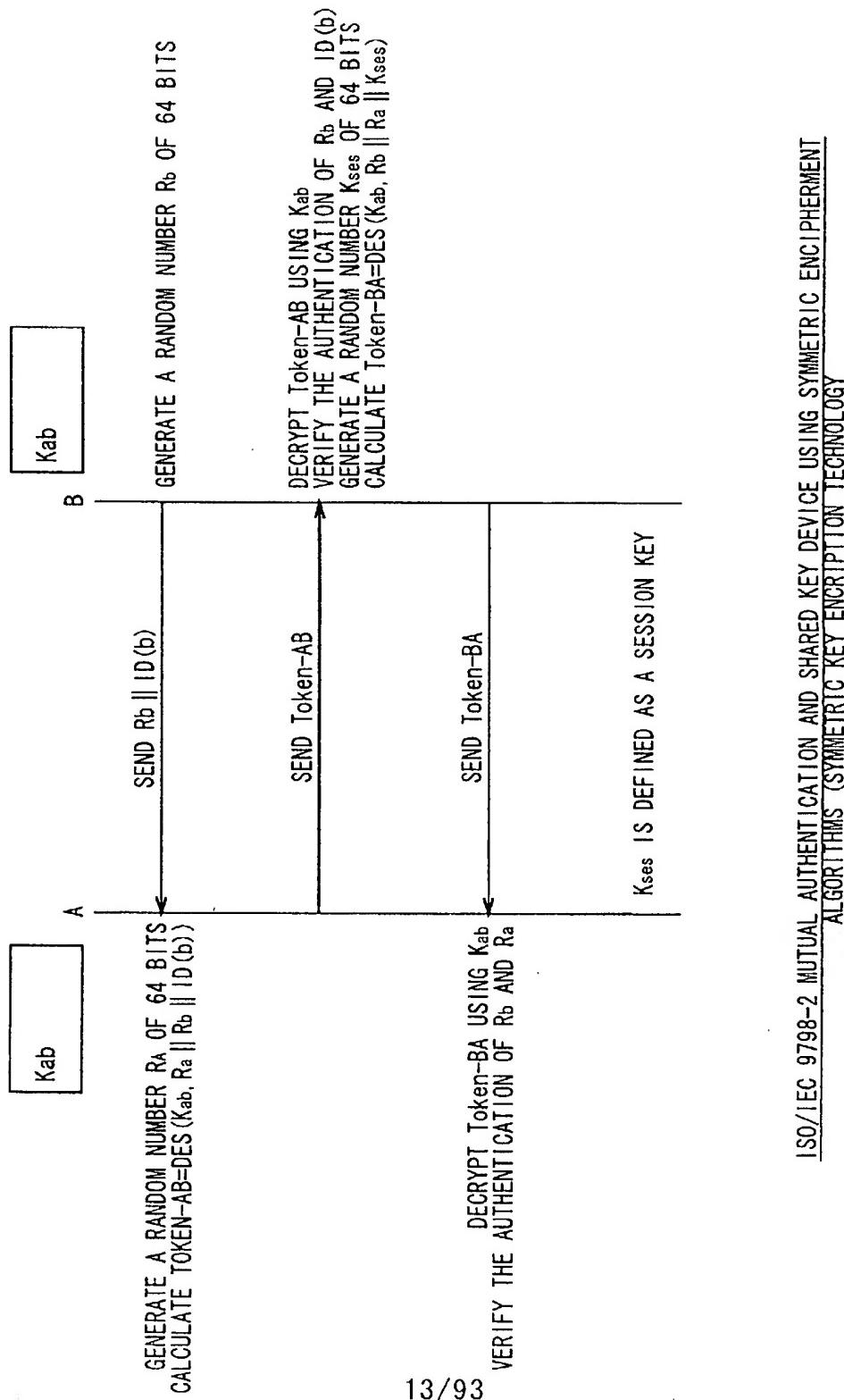
FIG. 11

AUTHENTICATION OF SIGNATURE

AUTHENTICATION OF SIGNATURE (IEEE P1363/D3)

FIG. 12

09/937410



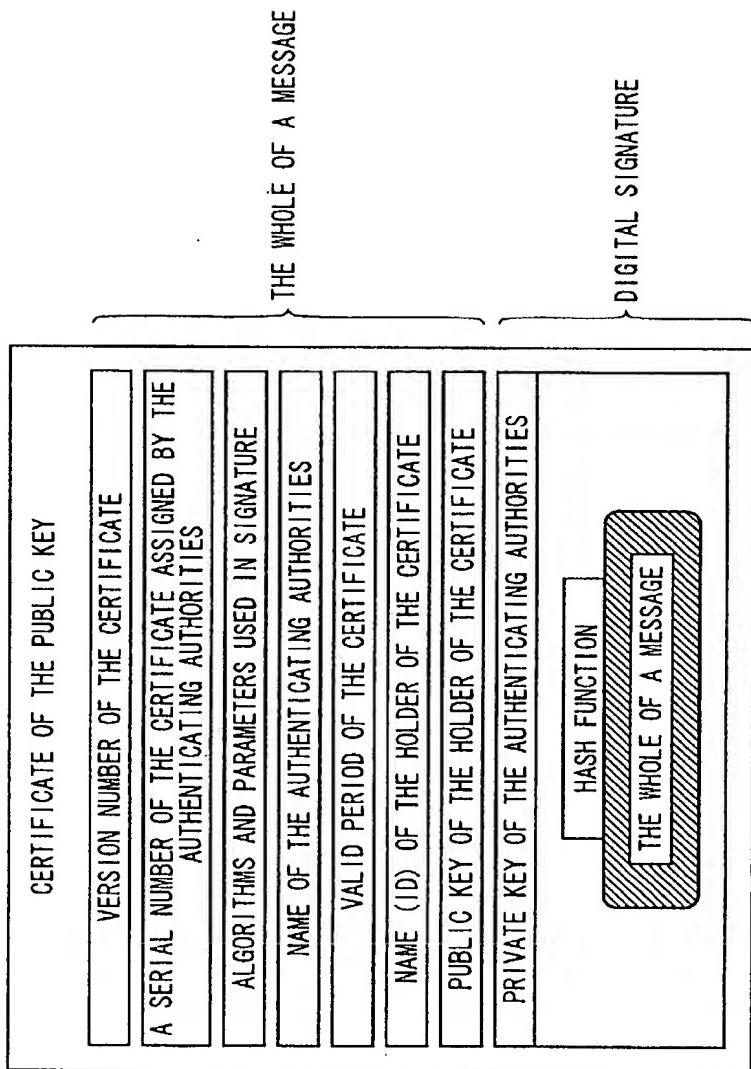
13/93

ISO/IEC 9798-2 MUTUAL AUTHENTICATION AND SHARED KEY DEVICE USING SYMMETRIC ENCIPHERMENT
ALGORITHMS (SYMMETRIC KEY ENCRYPTION TECHNOLOGY)

FIG. 13

09/937410

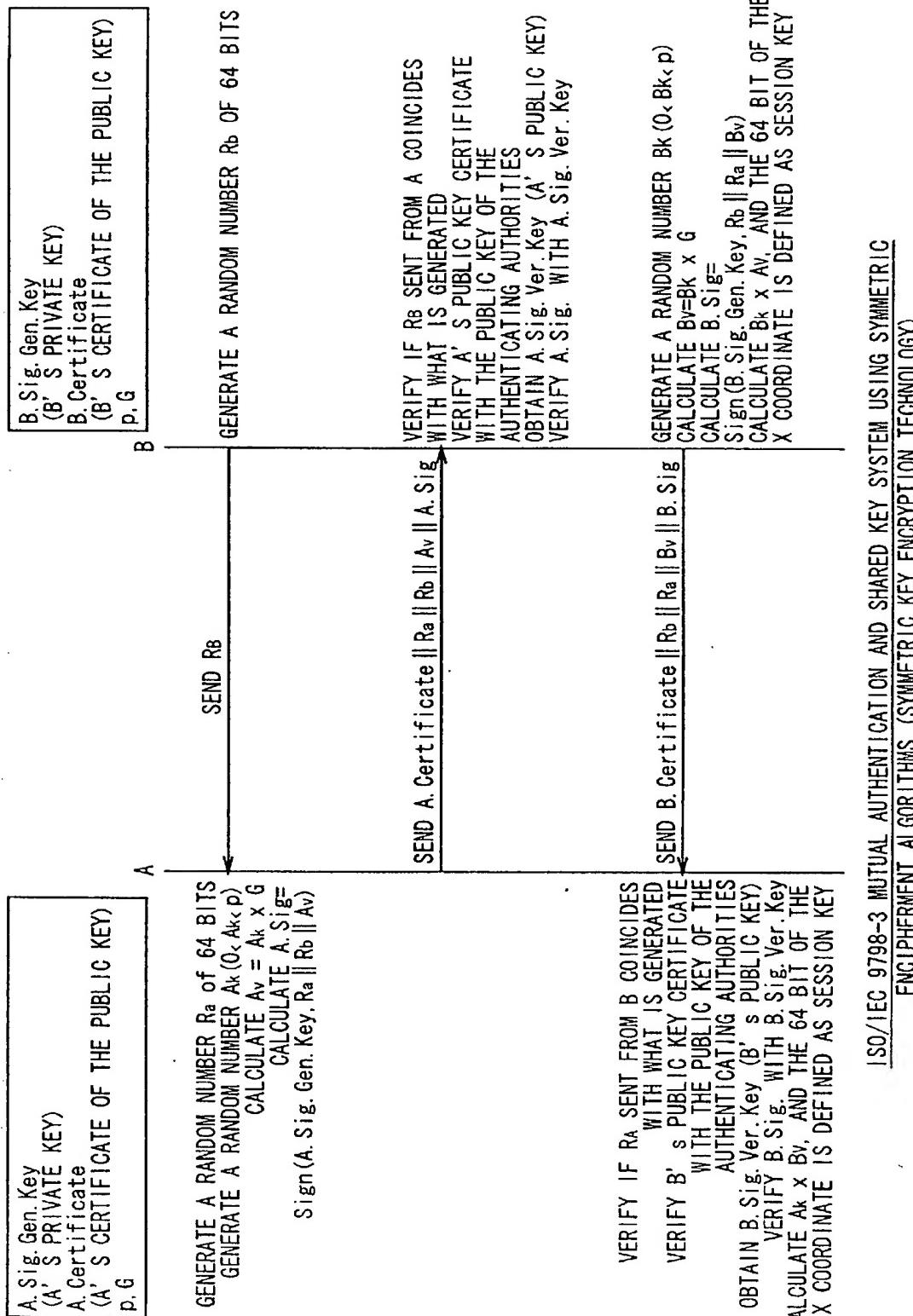
FORMAT "CERTIFICATE



CERTIFICATE OF PUBLIC KEY

FIG. 14

09/937410

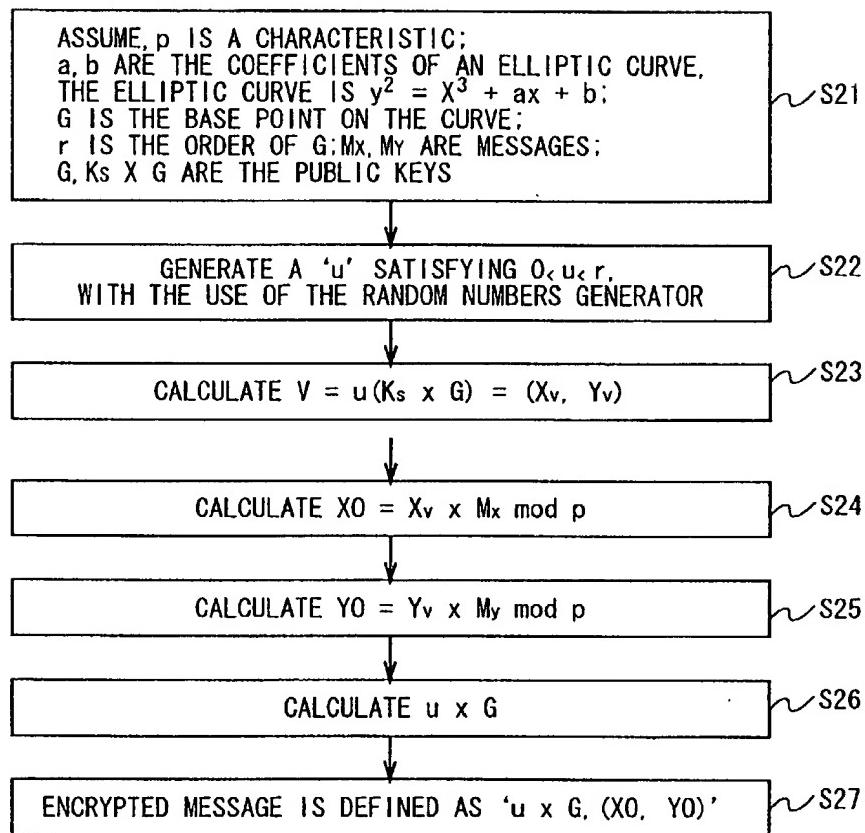


15/93

FIG. 15

09 / 937410

ENCRYPTION



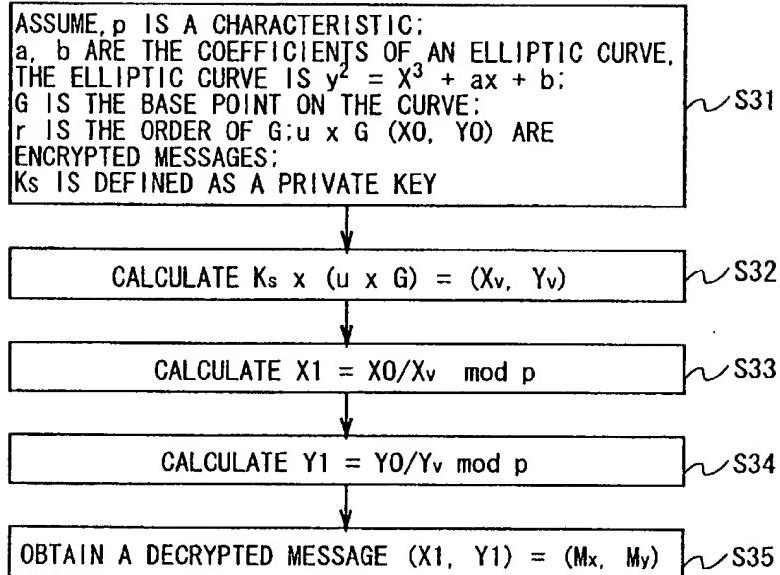
ENCRYPTION USING ELLIPTIC CURVE ENCRYPTION METHOD (MENEZES-VANSTONE)

FIG. 16

09/93741U

TOP SECRET//COMINT

DECRYPTION

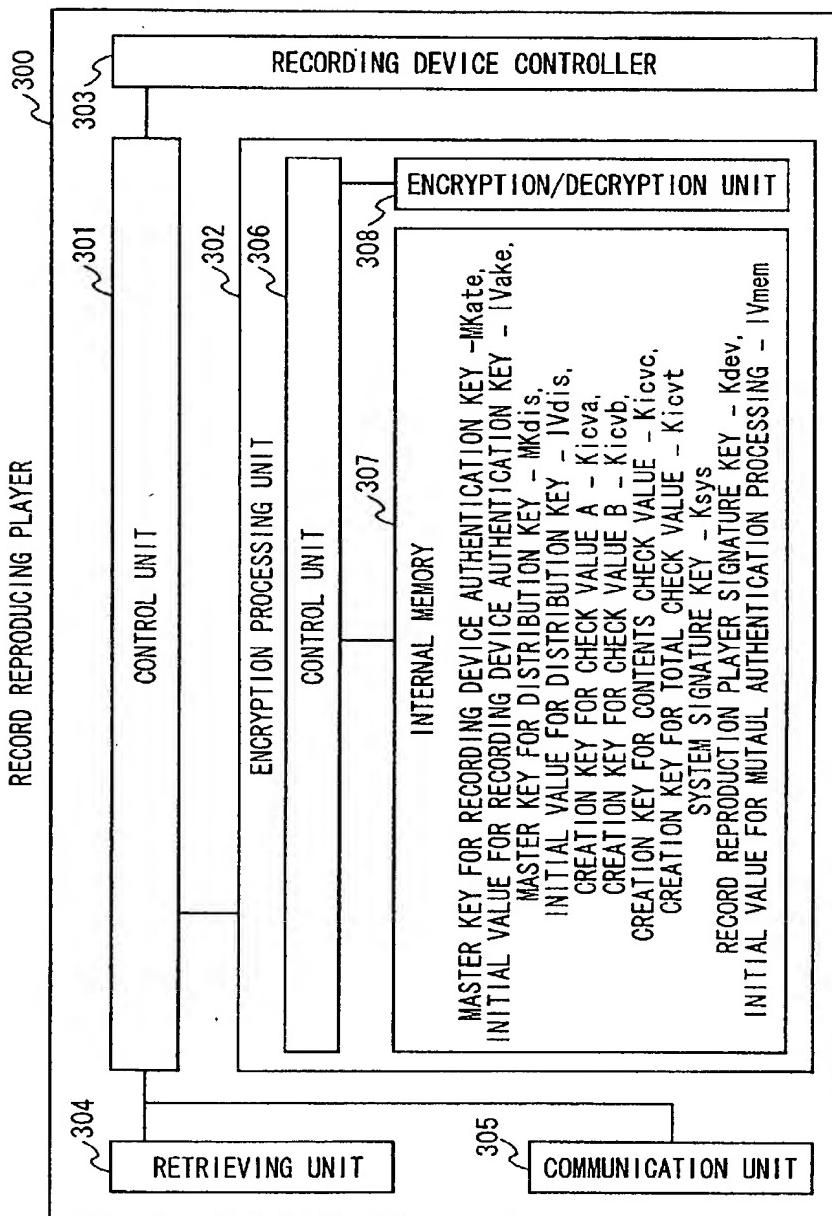


DECRYPTION USING ELLIPTIC CURVE ENCRYPTION MTHOD (MENEZES-VANSTONE)

FIG. 17

17/93

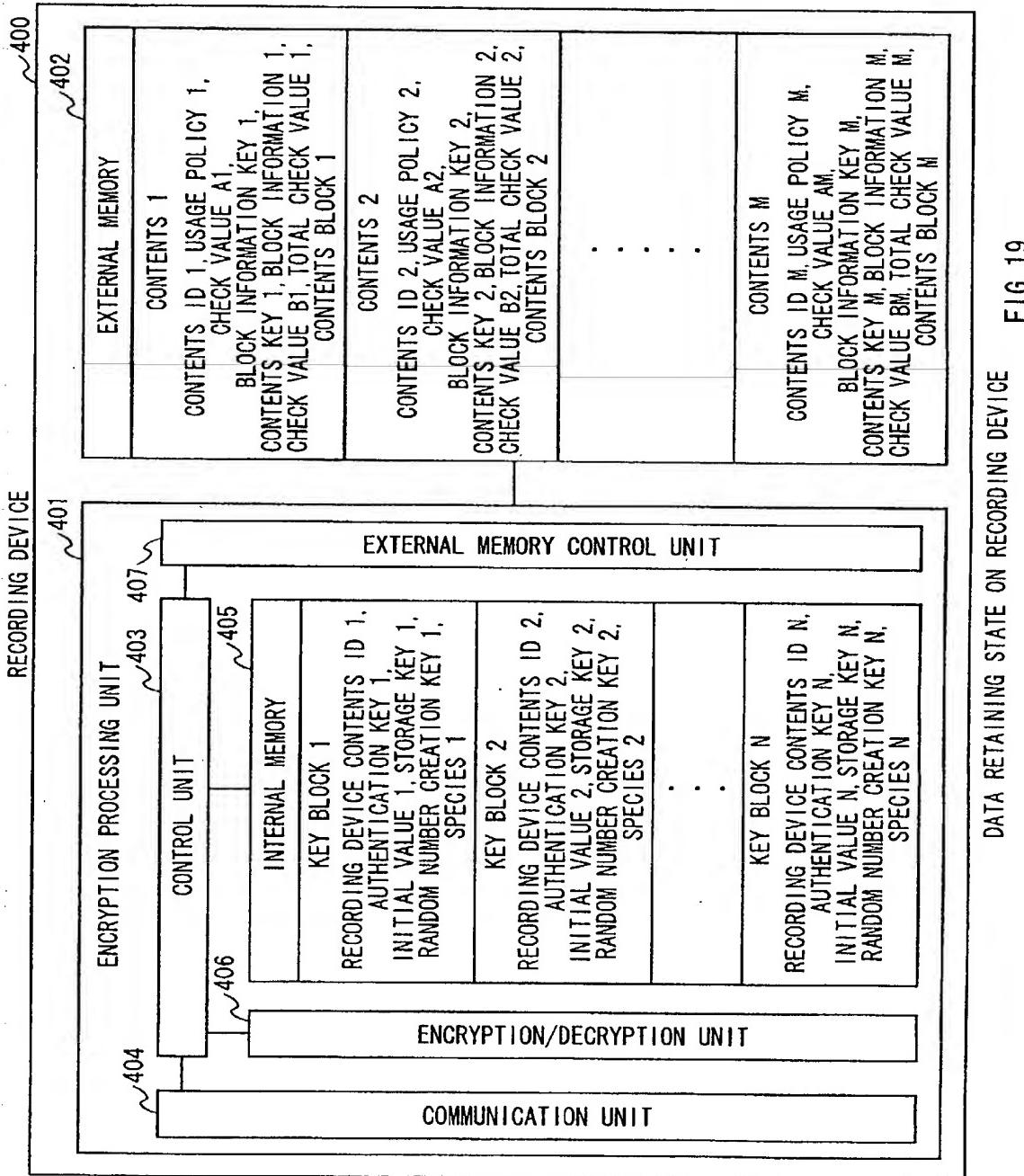
09/937410



DATA RETAINING STATE ON RECORD REPRODUCING PLAYER

FIG. 18

09/937410

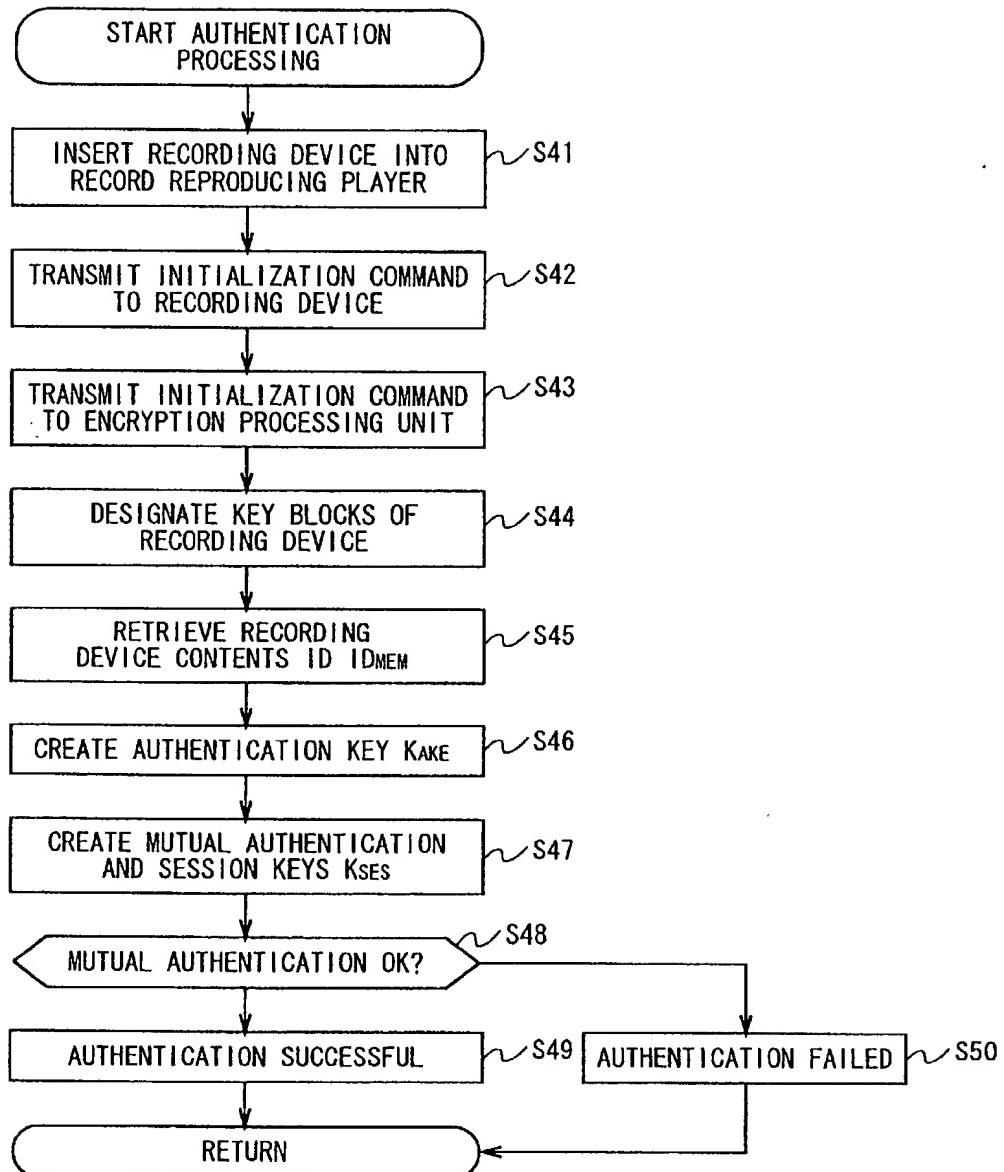


DATA RETAINING STATE ON RECORDING DEVICE

FIG. 19

09/937410

FOURTY-FOUR-660



MUTUAL AUTHENTICATION BETWEEN RECORD REPRODUCTION AND RECORDING DEVICE

FIG. 20

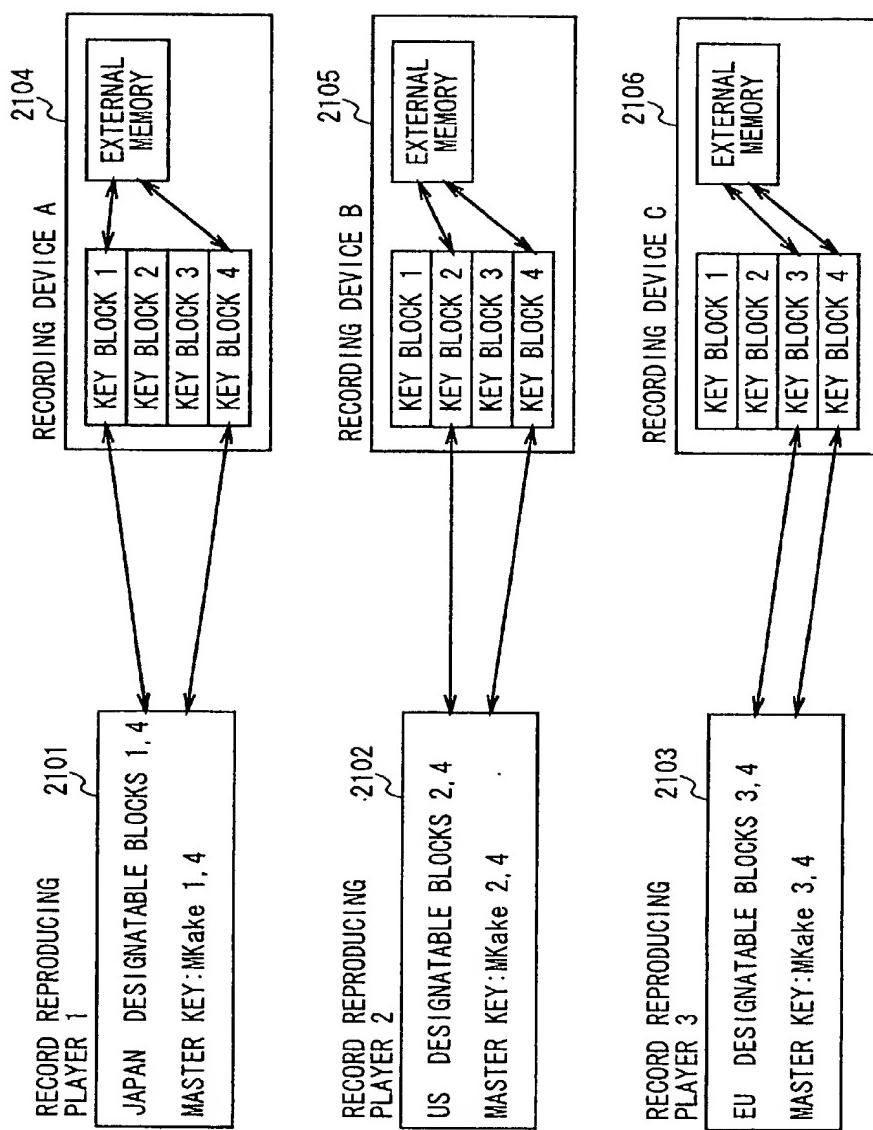
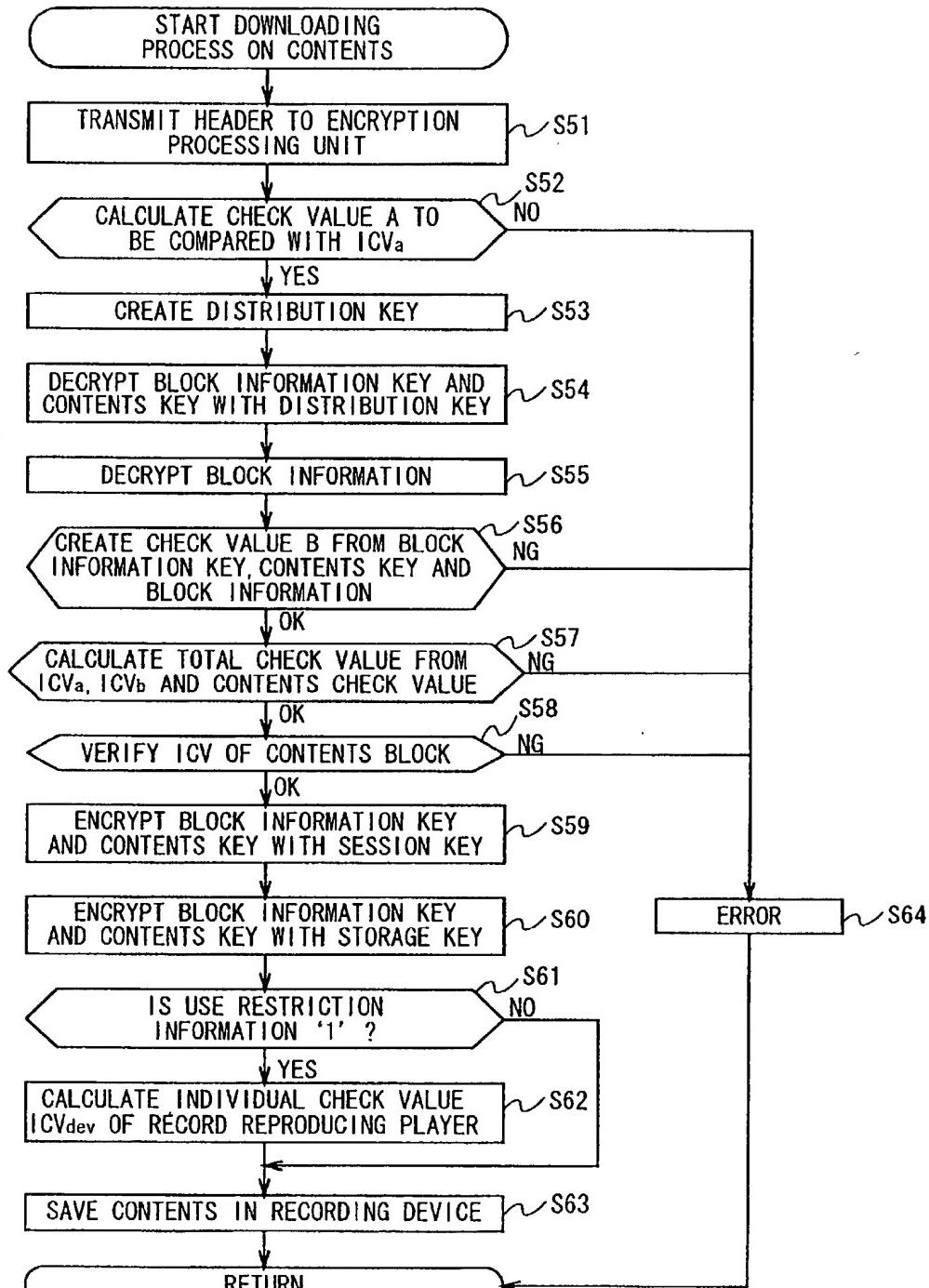


FIG. 21

09/937410

TOP SECRET - OFFICE OF THE CHIEF OF STAFF

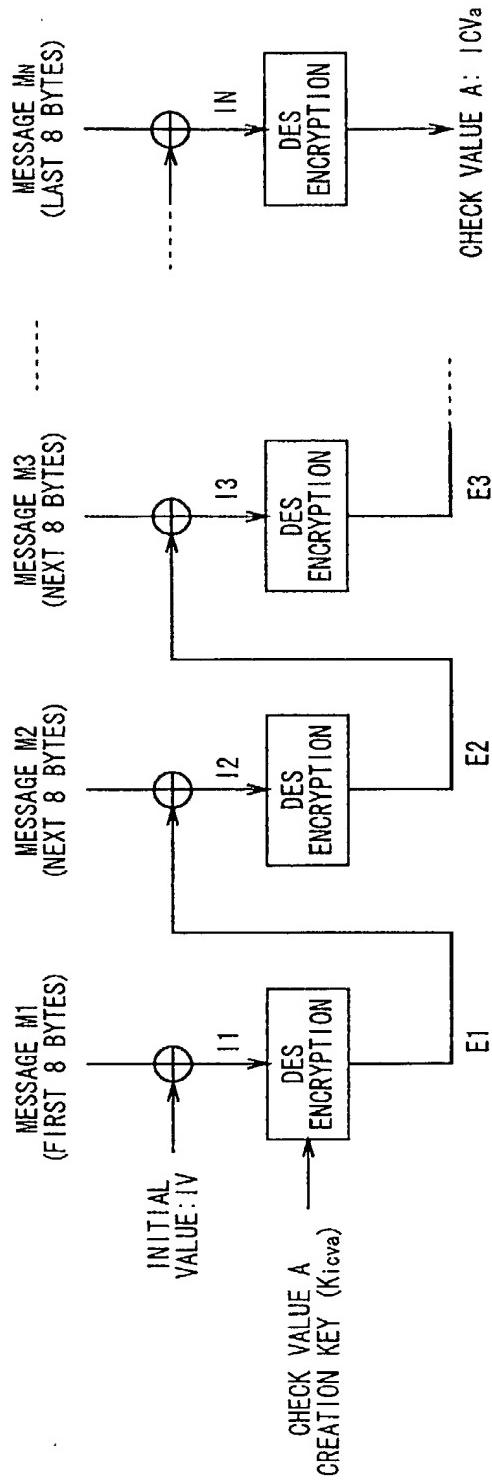


DOWNLOADING PROCESS OF CONTENTS

FIG. 22

22/93

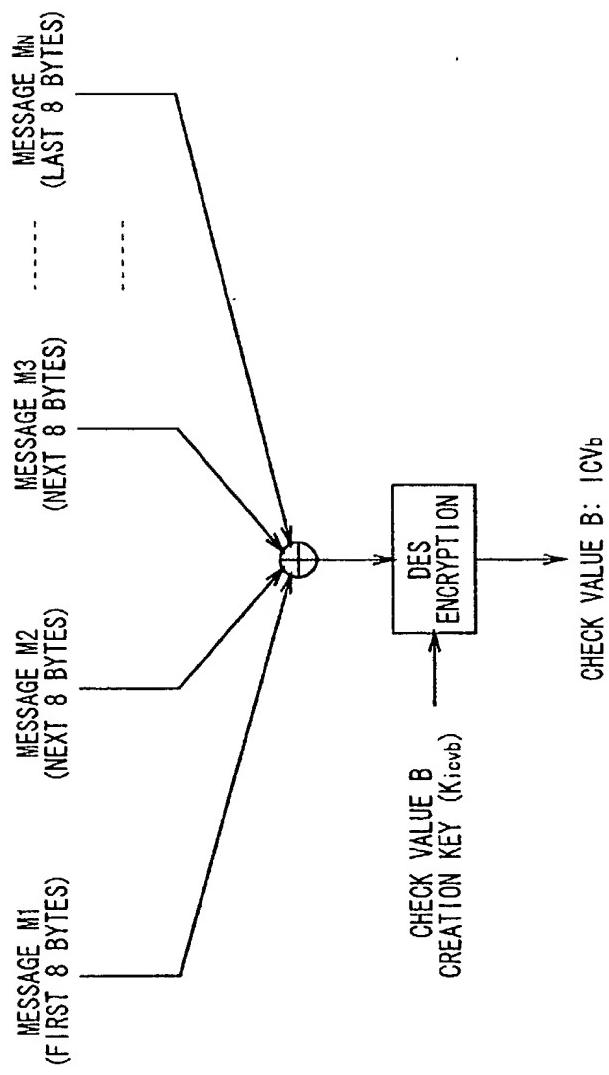
09/937410



MESSAGE M₁ - MN: CONTENTS ID, USAGE POLICY
 \oplus :EXCLUSIVE OR (XOR) PROCESS (8-BYTE UNIT)

FIG. 23

09/937410



MESSAGE M1 - Mn: BLOCK INFORMATION KEY Kbit, CONTENTS KEY Kcon, BLOCK INFORMATION
 \oplus : EXCLUSIVE OR (XOR) PROCESS (8-BYTE UNIT)

FIG. 24

TOURIST DIFFERENCE

09/937410

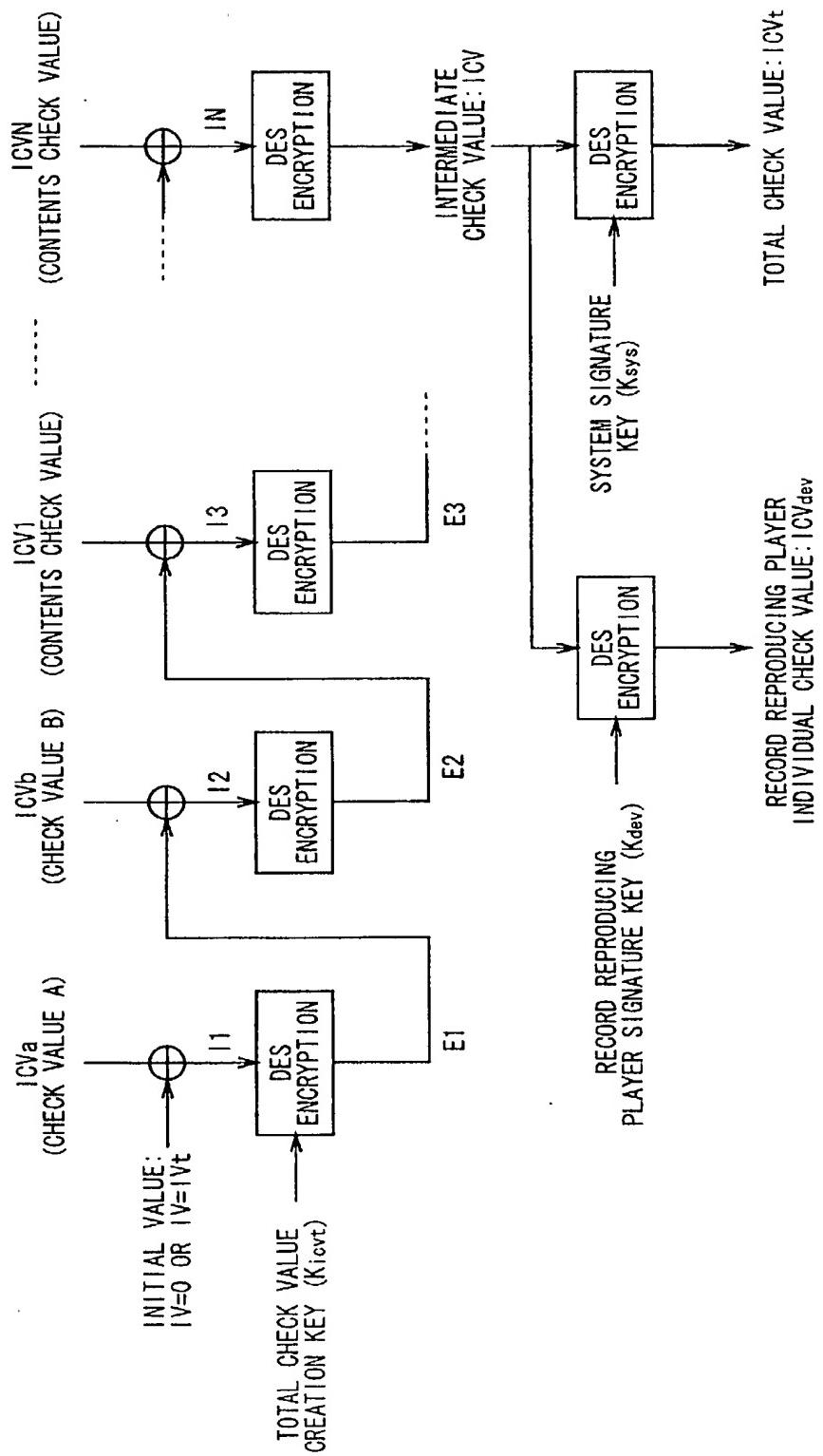


FIG. 25

09/937410

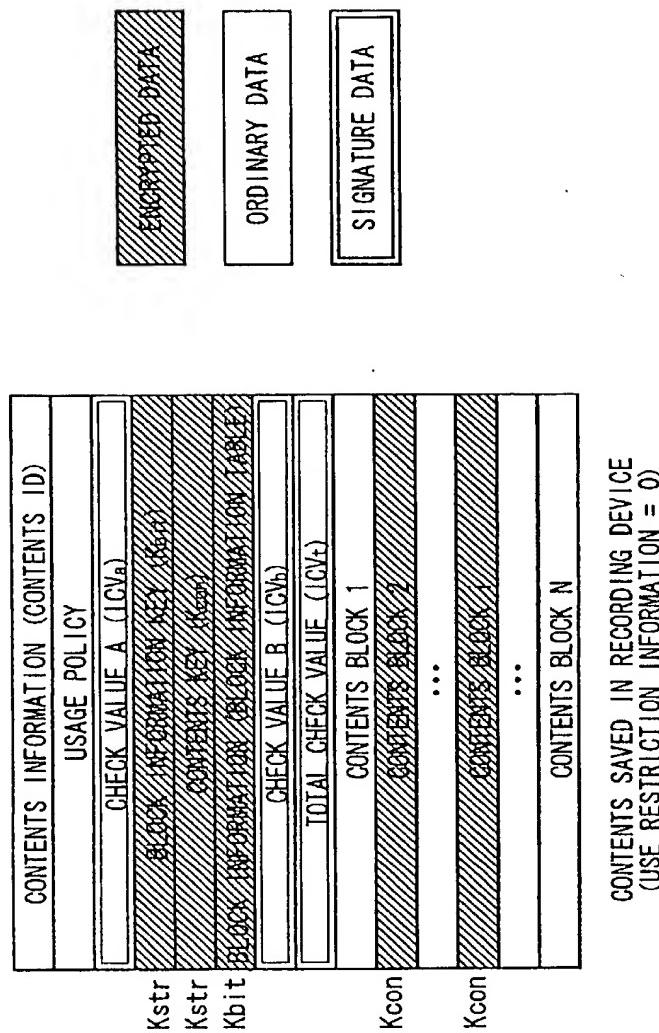


FIG. 26

09/937410

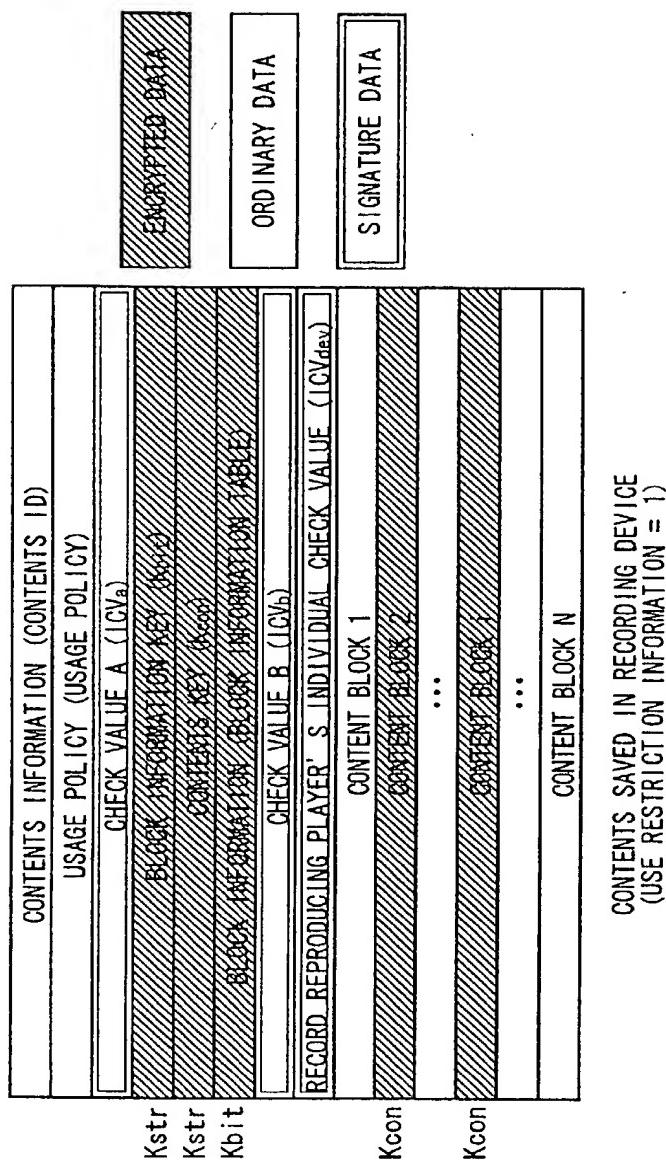


FIG. 27

TOP SECRET - GREECE 600

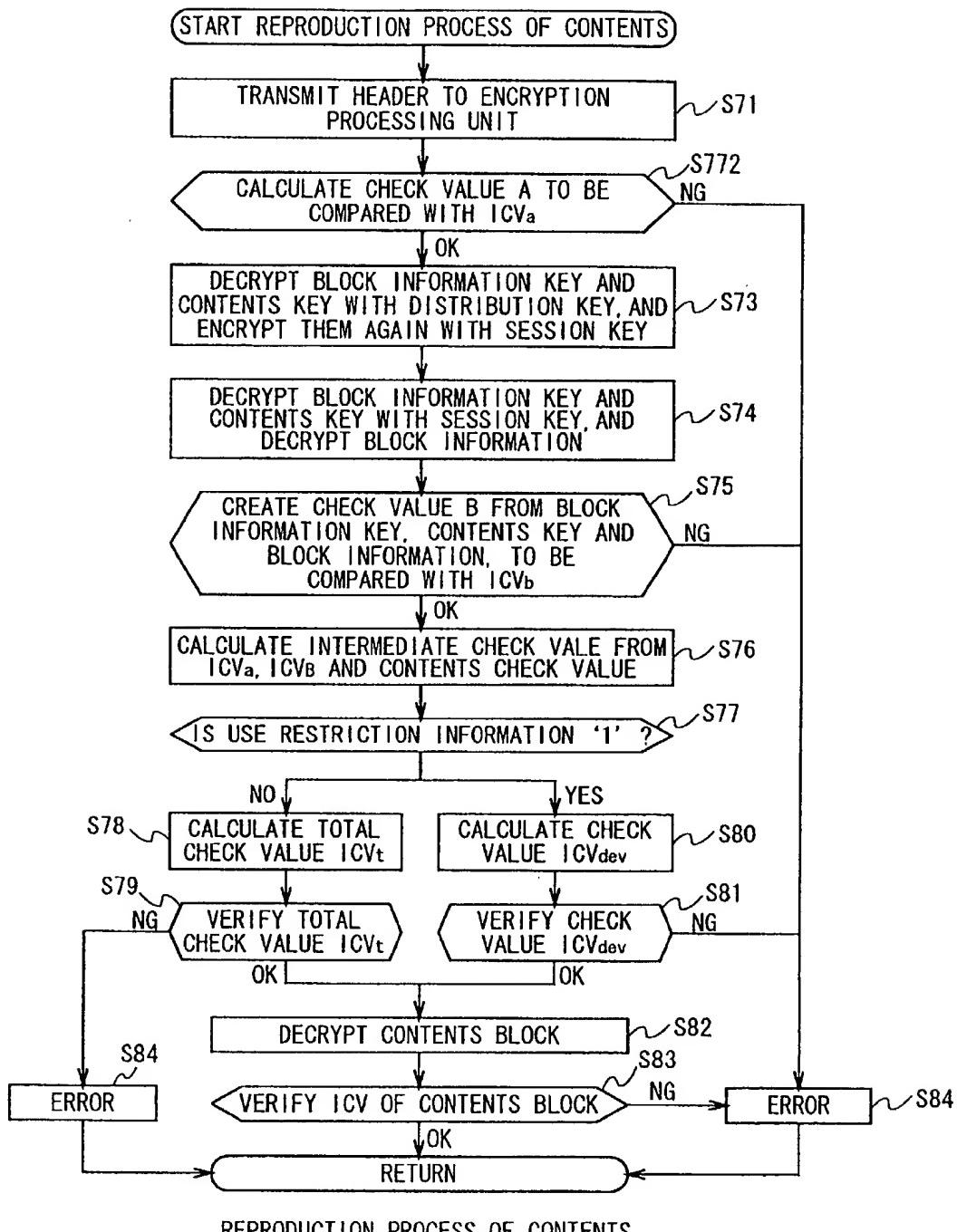


FIG. 28

09/937410

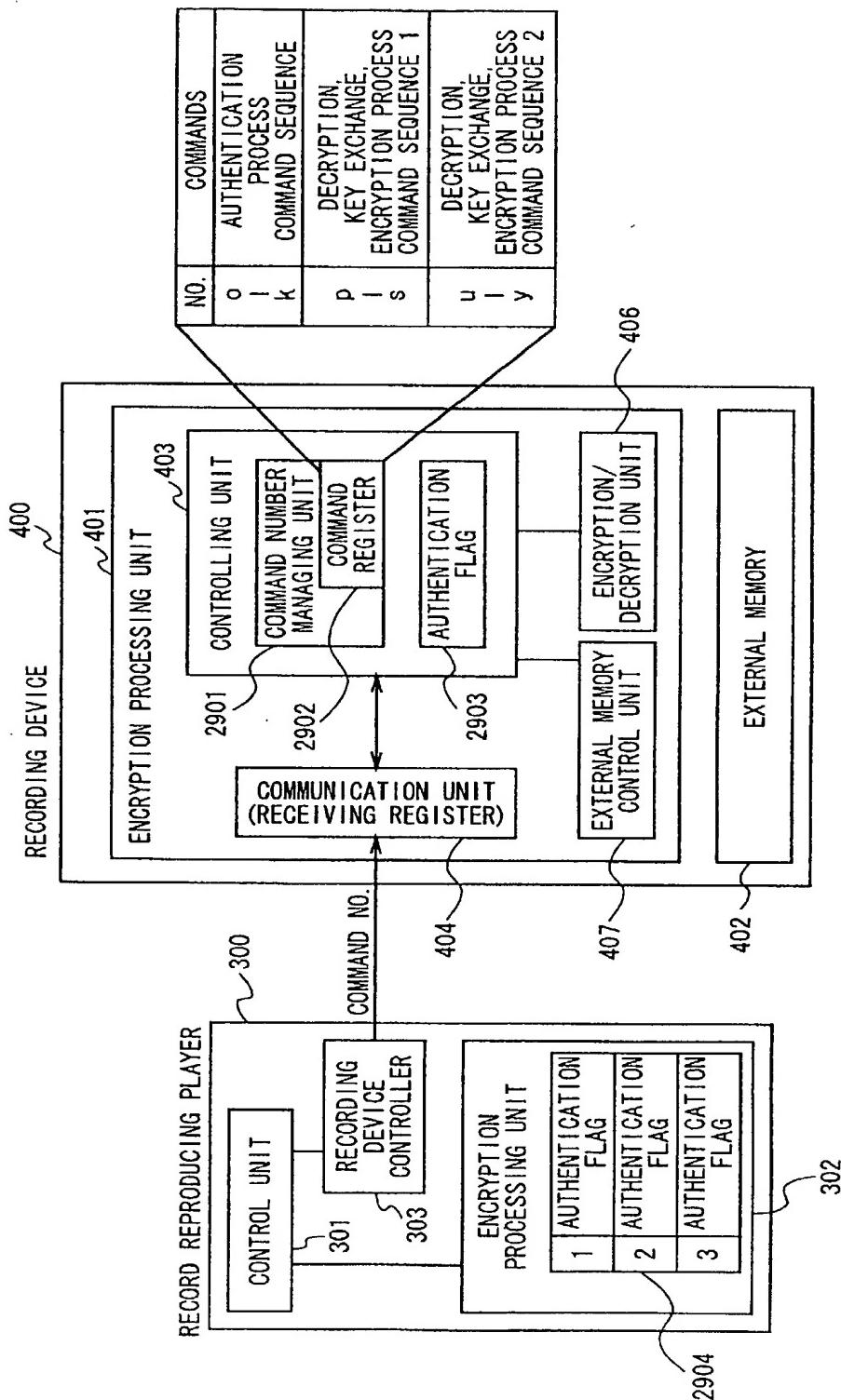


FIG. 29

TOP SECRET - OFFICE OF THE SECRETARY OF DEFENSE

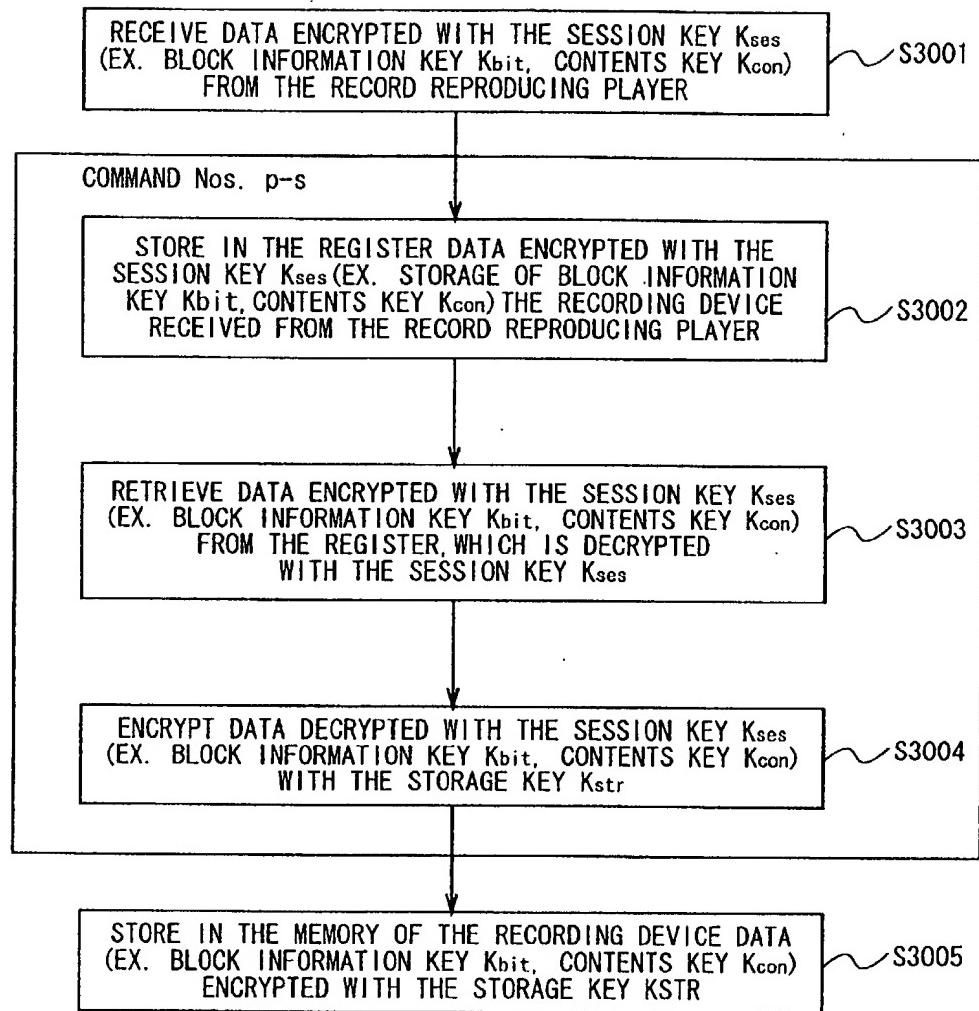


FIG. 30

TOP SECRET OFFICE 26660

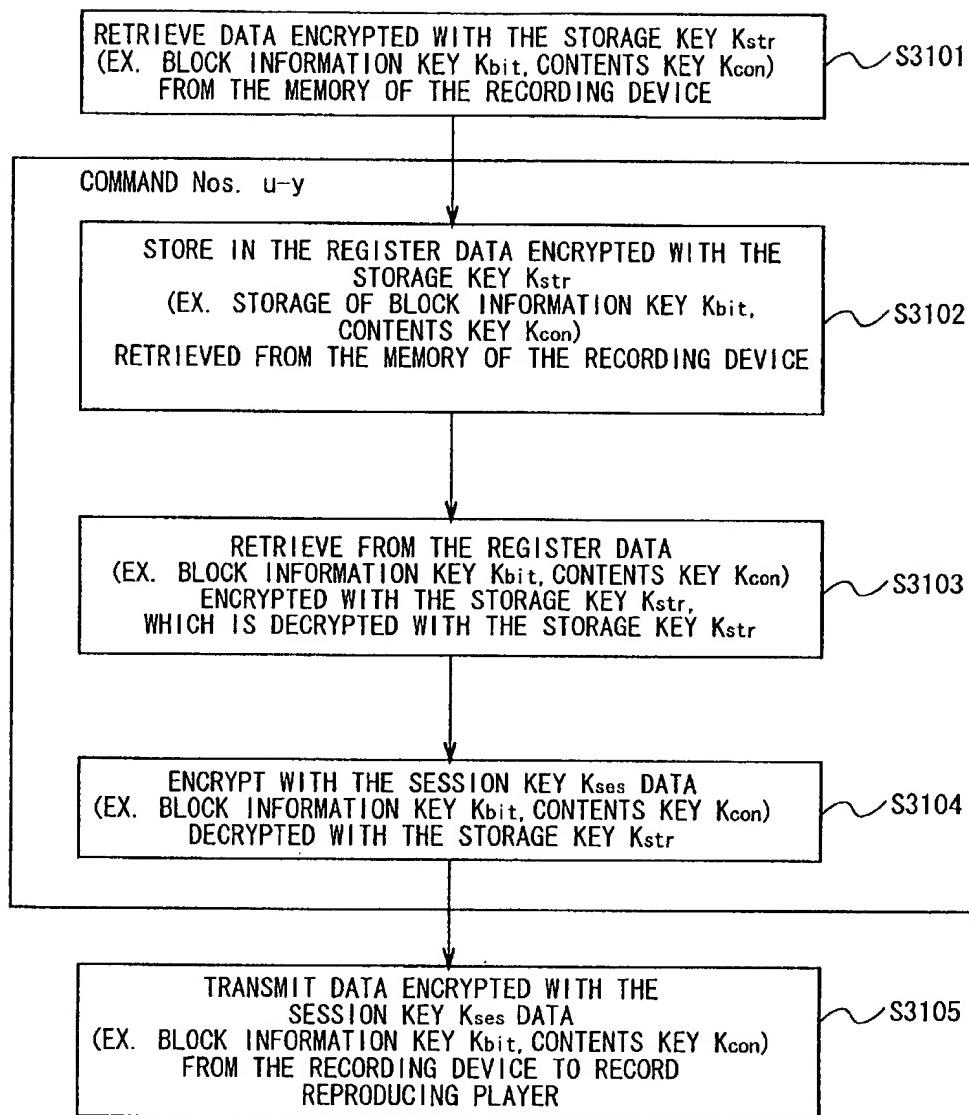


FIG. 31

09/937410

FORMAT TYPE 0

Kdis	CONTENTS INFORMATION (CONTENTS ID)
Kdis	USAGE POLICY (USAGE POLICY)
Kdis	CHECK VALUE A (ICVa)
Kdis	BLOCK INFORMATION TABLE
Kbit	CHECK VALUE B (ICVb)
Kcon	TOTAL CHECK VALUE (ICVt)
Kcon	INDIVIDUAL CHECK VALUE (ICVdev)
Kcon	CONTENTS BLOCK 2
Kcon	CONTENTS BLOCK i
	...
	CONTENTS BLOCK N

DATA FORMAT ON MEDIA AND COMMUNICATION ROUTE

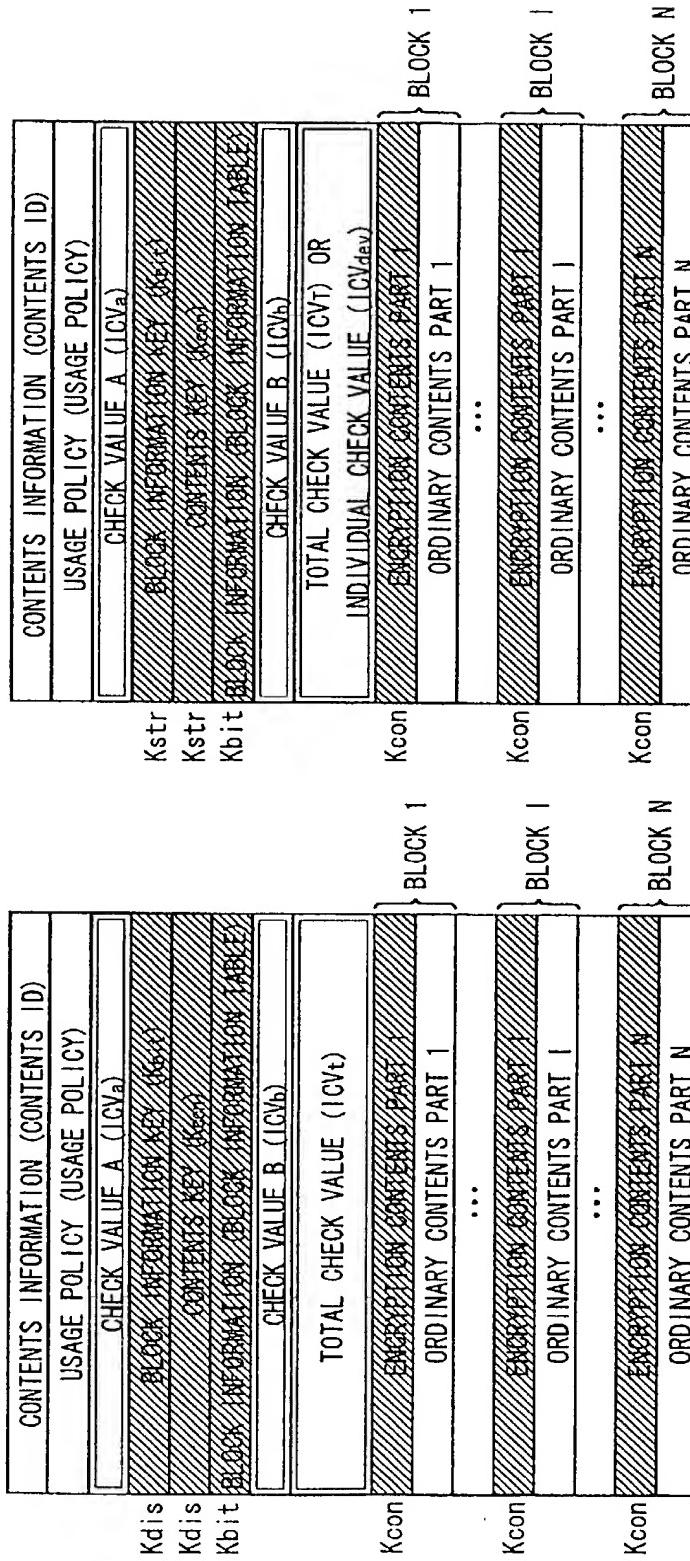


CONTENTS SAVED ON RECORDING DEVICE

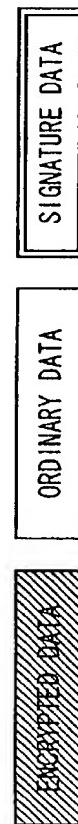


Kstr	CONTENTS INFORMATION (CONTENTS ID)
Kstr	USAGE POLICY (USAGE POLICY)
Kstr	CHECK VALUE A (ICVa)
Kstr	BLOCK INFORMATION TABLE
Kbit	CHECK VALUE B (ICVb)
Kcon	TOTAL CHECK VALUE (ICVt) OR
Kcon	INDIVIDUAL CHECK VALUE (ICVdev)
Kcon	CONTENTS BLOCK 2
Kcon	CONTENTS BLOCK i
	...
	CONTENTS BLOCK N

FIG. 32

FORMAT TYPE 1

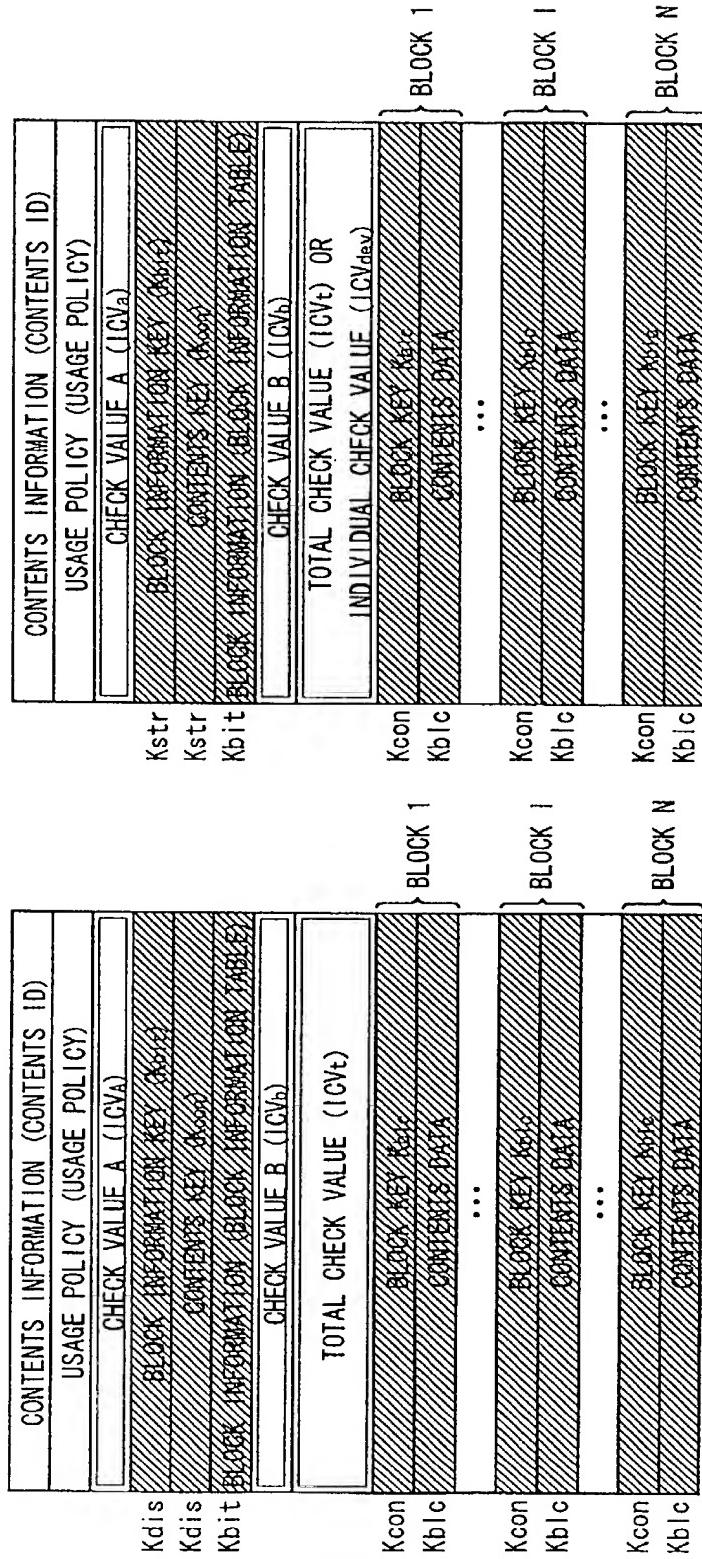
DATA FORMAT ON MEDIA AND COMMUNICATION ROUTE



CONTENTS SAVED ON RECORDING DEVICE

FIG. 33

09/937410

FORMAT TYPE 2

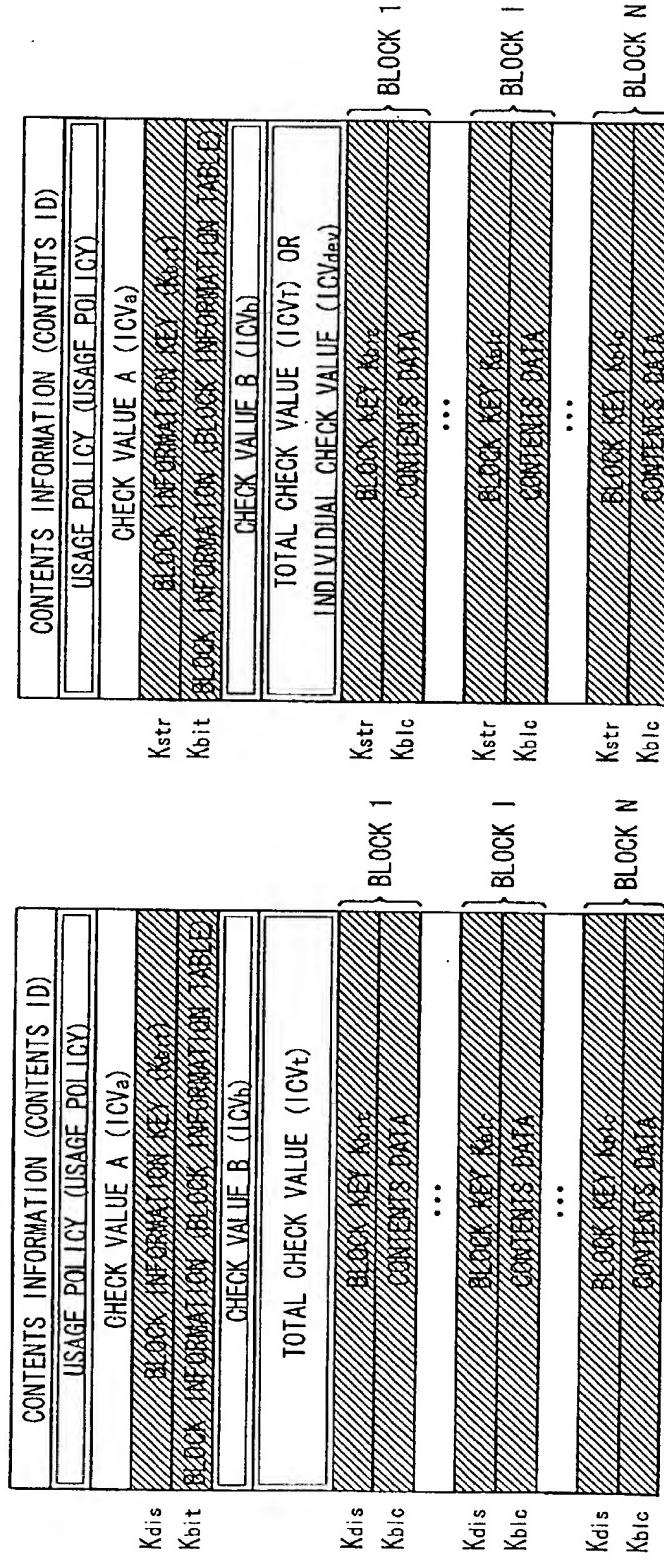
DATA FORMAT ON MEDIA AND COMMUNICATION ROUTE

CONTENTS SAVED ON RECORDING DEVICE

FIG. 34

09/937410

FORMAT TYPE 3



35/93

DATA FORMAT ON MEDIA AND COMMUNICATION ROUTE

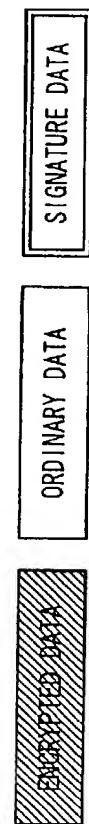
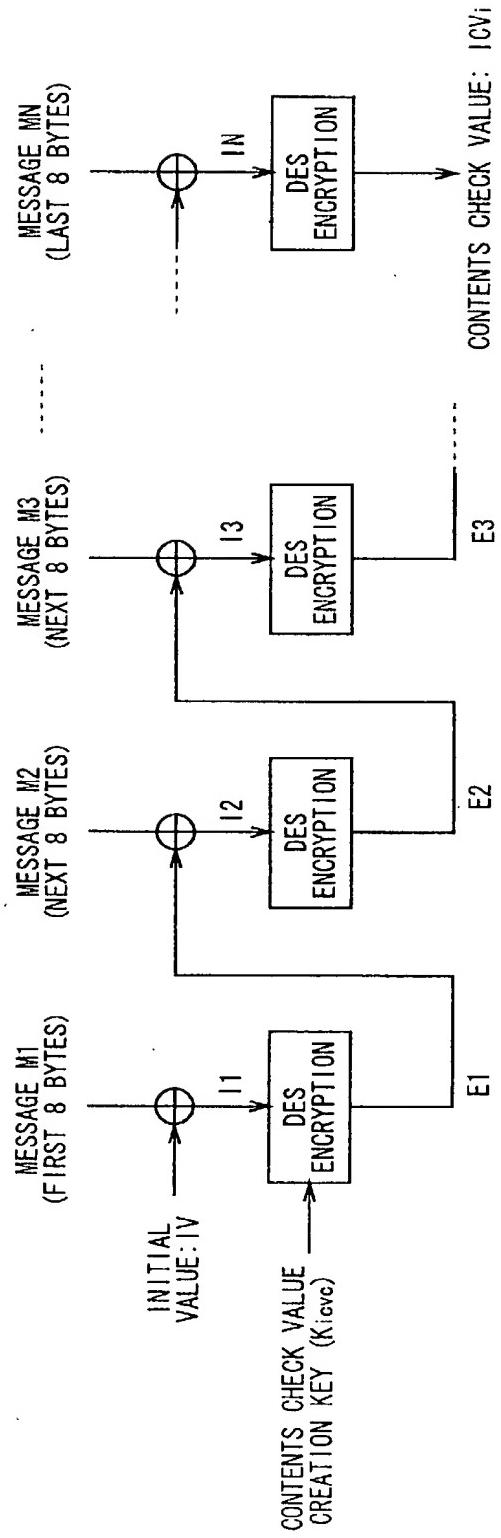


FIG. 35

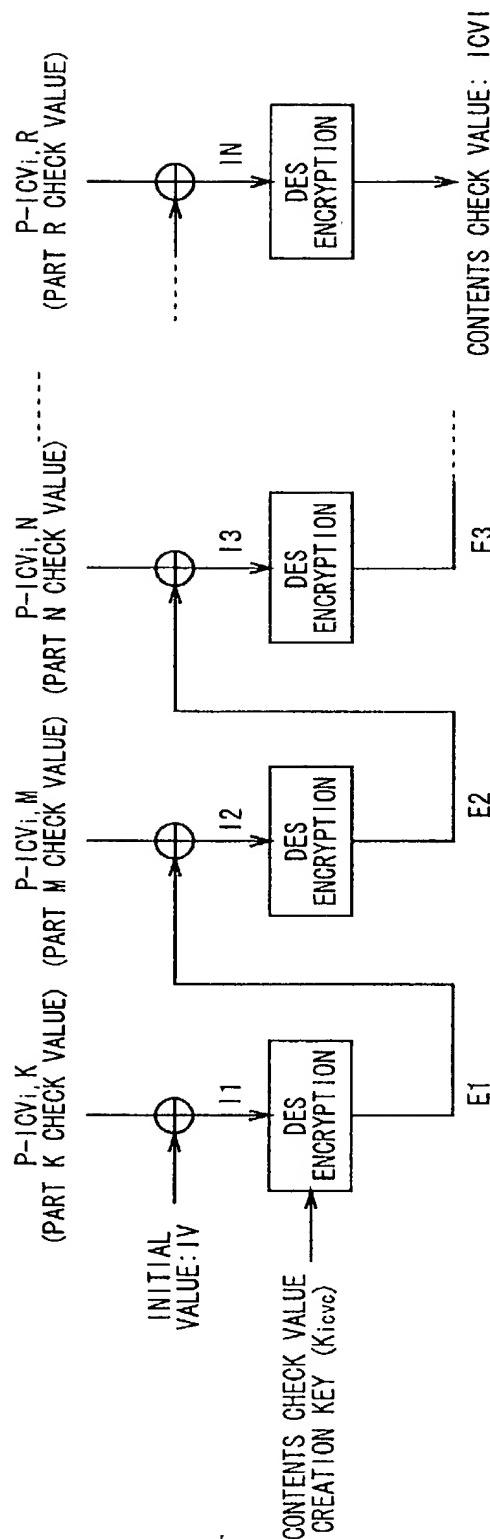
TO CRYPT = DATA CEC E660

09/937410



MESSAGE M1 - MN: CONTENTS DATE OF CONTENTS |
⊕ EXCLUSIVE OR (XOR) PROCESS (8-BYTE UNIT)

FIG. 36



⊕: EXCLUSIVE OR (XOR) PROCESS (8-BYTE UNIT)

09/937410

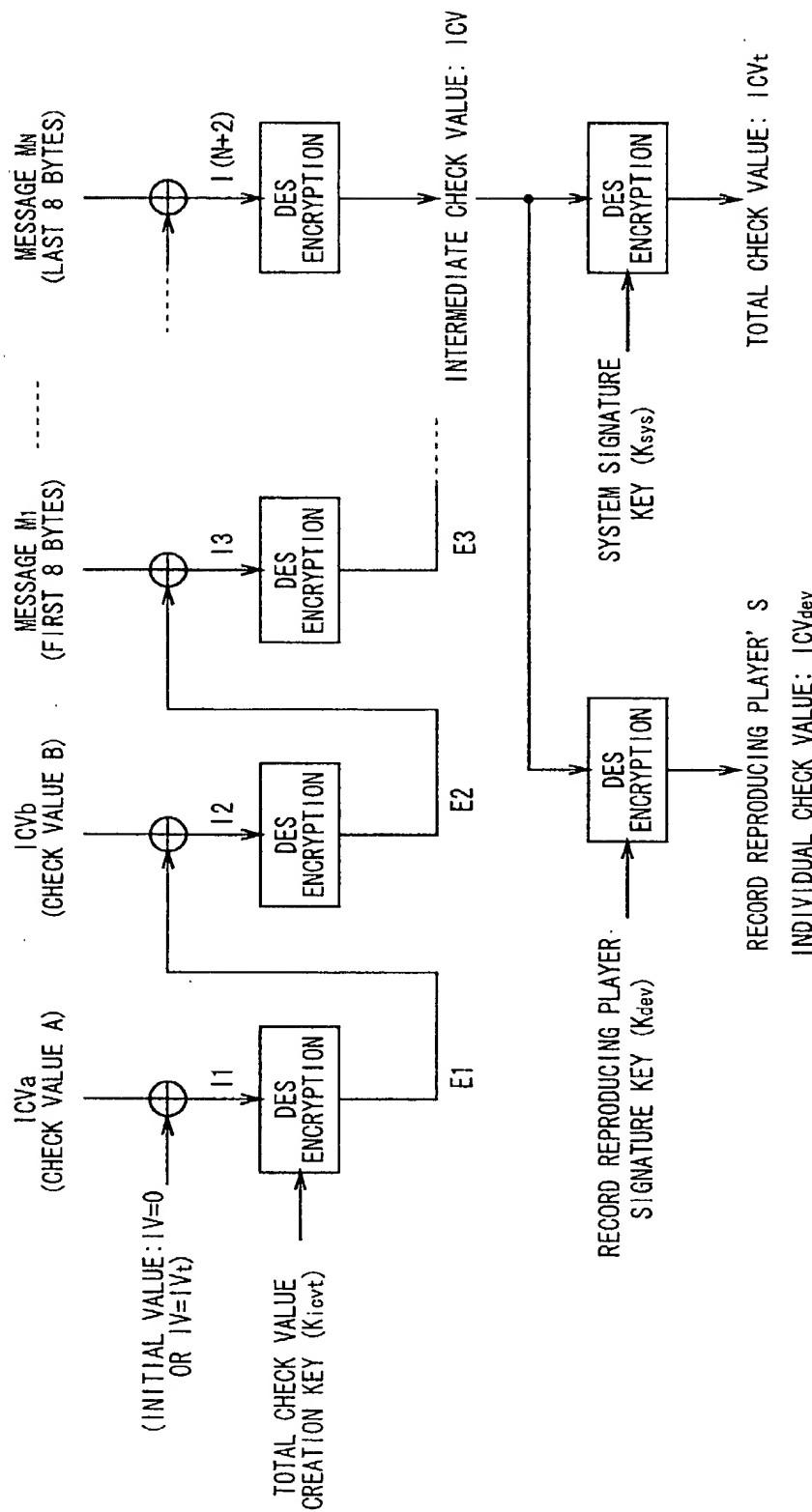


FIG. 38

MESSAGE $M_1 - M_N$: DATA OF CONTENTS BLOCK 1 ~ N
 \oplus : EXCLUSIVE OR (XOR) PROCESS (8-BYTE UNIT)

FORMAT TYPE 0, 1 DOWNLOADING PROCESS

TOC/PFT-OFFICE6560

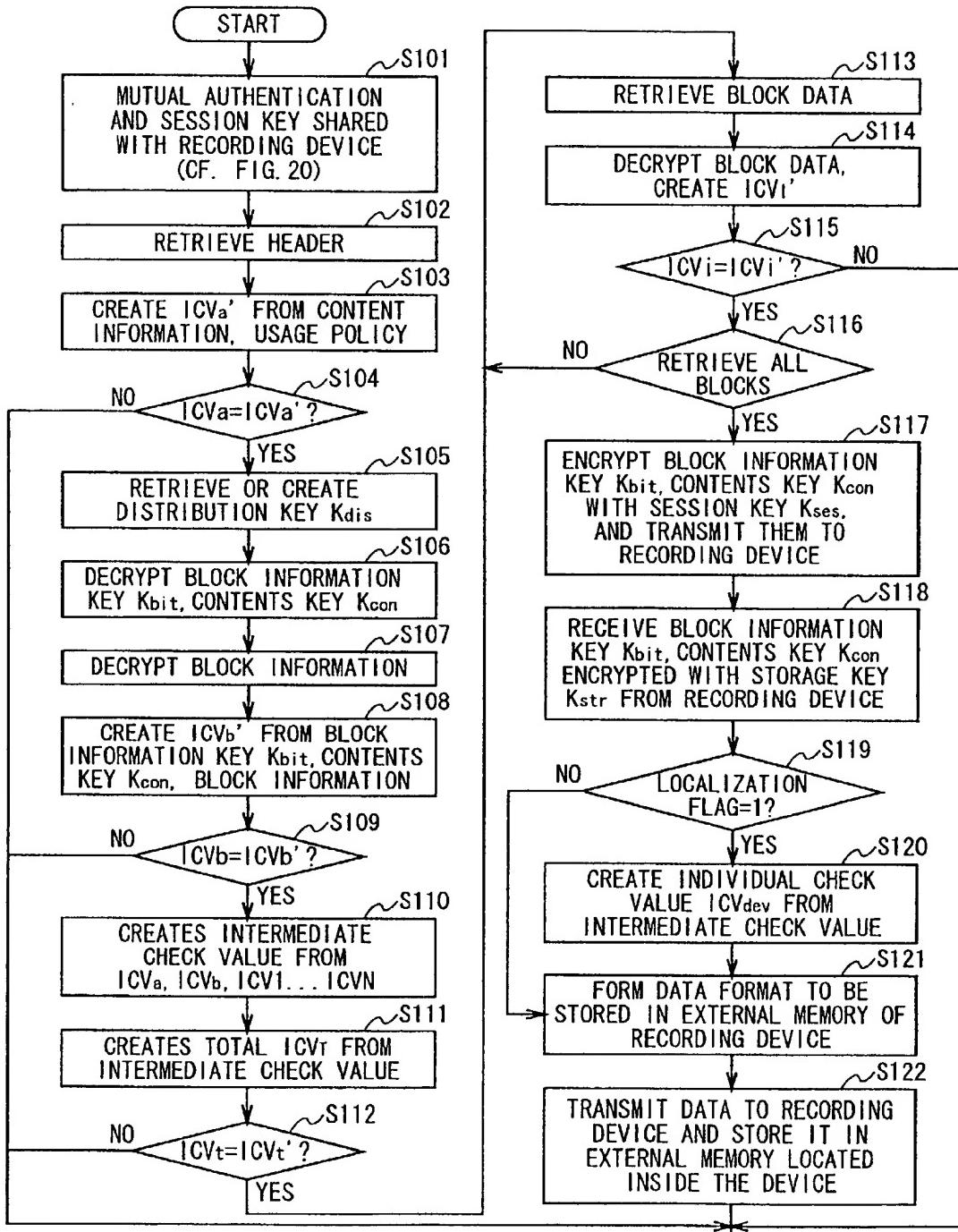


FIG. 39

FORMAT TYPE 2 DOWNLOADING PROCESS

TOP SECRET//REF ID: A660

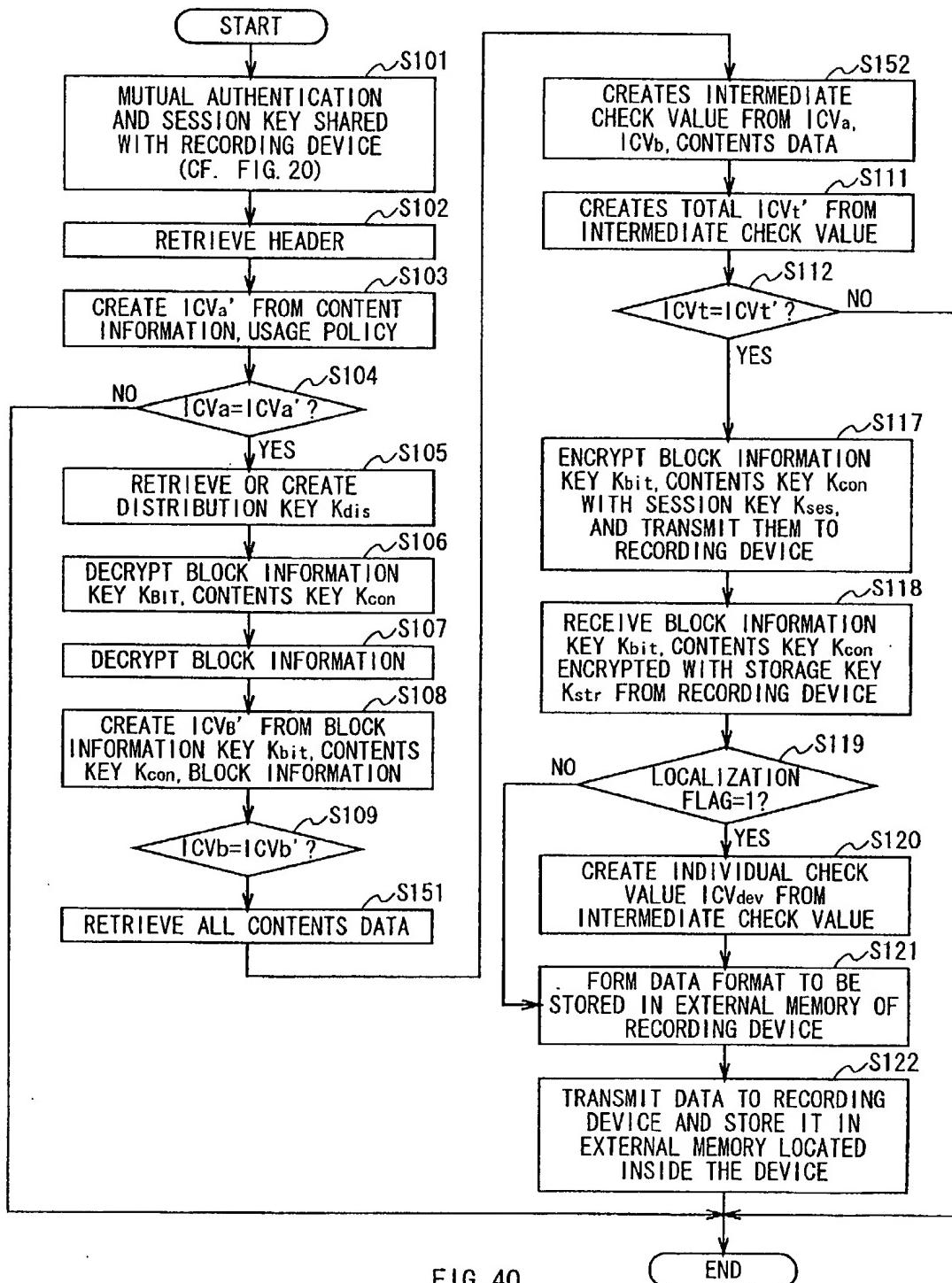


FIG. 40

FORMAT TYPE 3 DOWNLOADING PROCESS

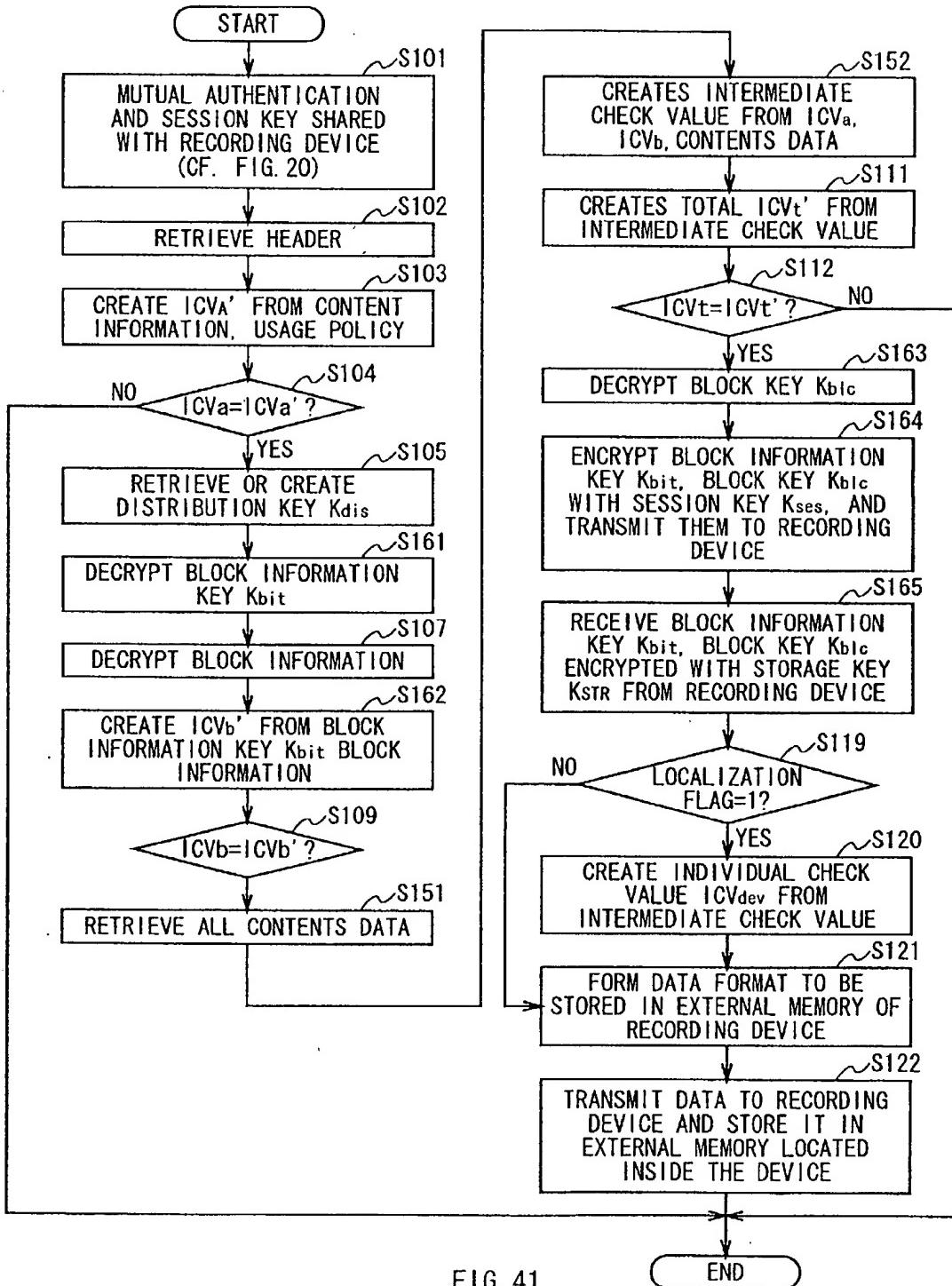


FIG. 41

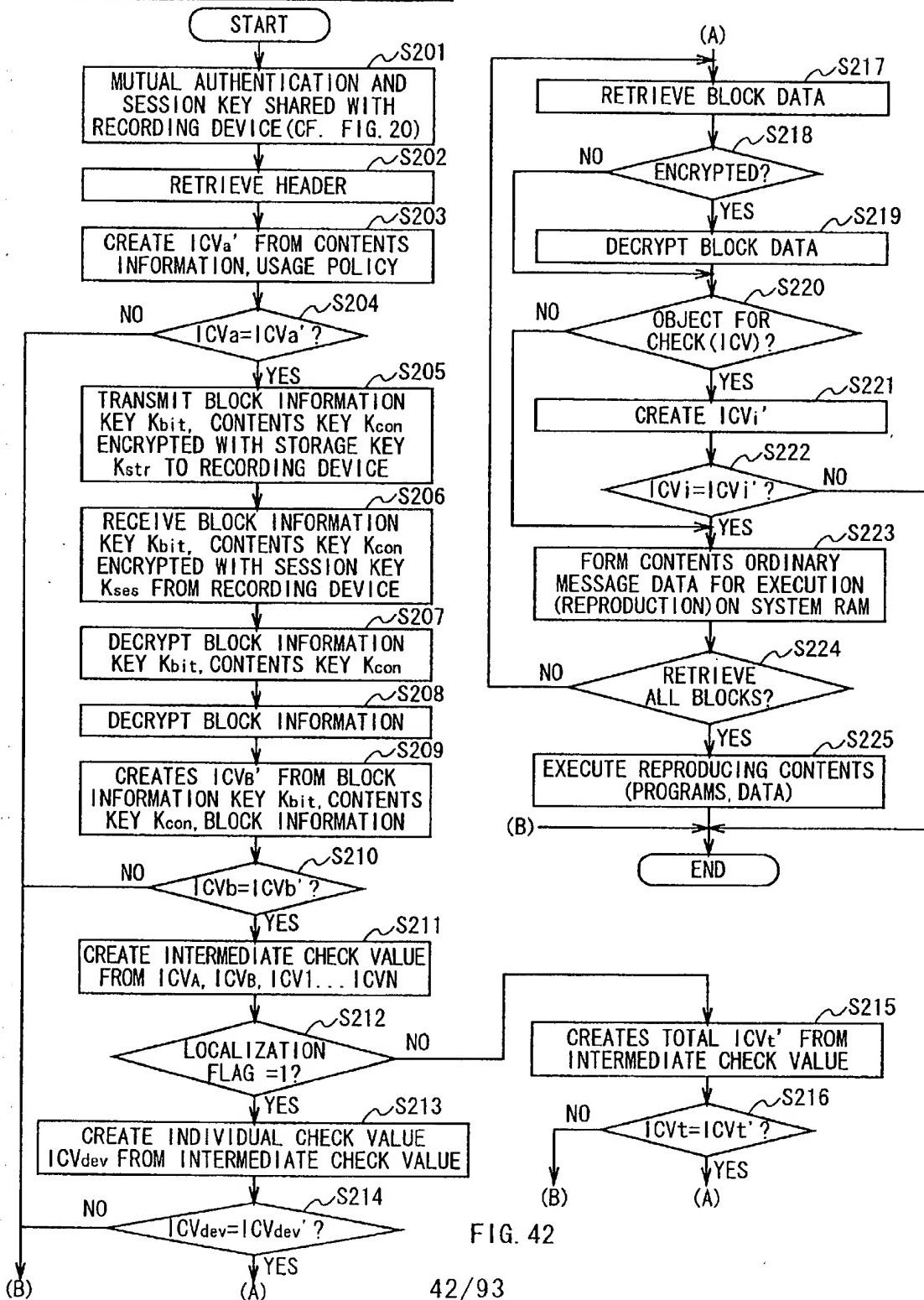
FORMAT TYPE 4 DOWNLOADING PROCESS

FIG. 42

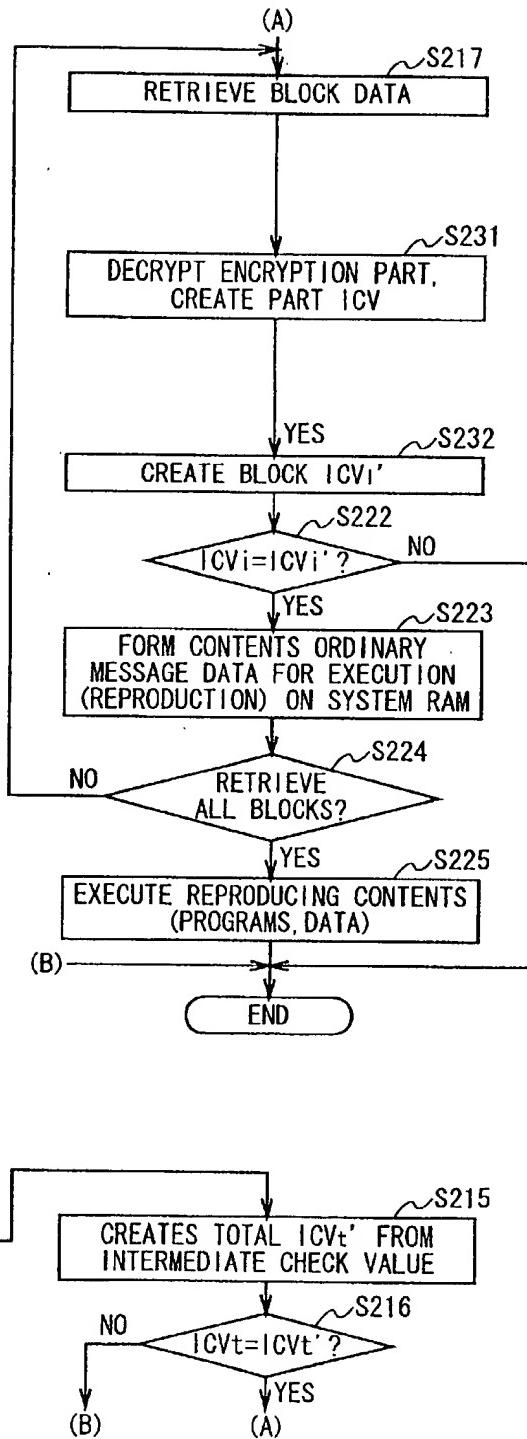
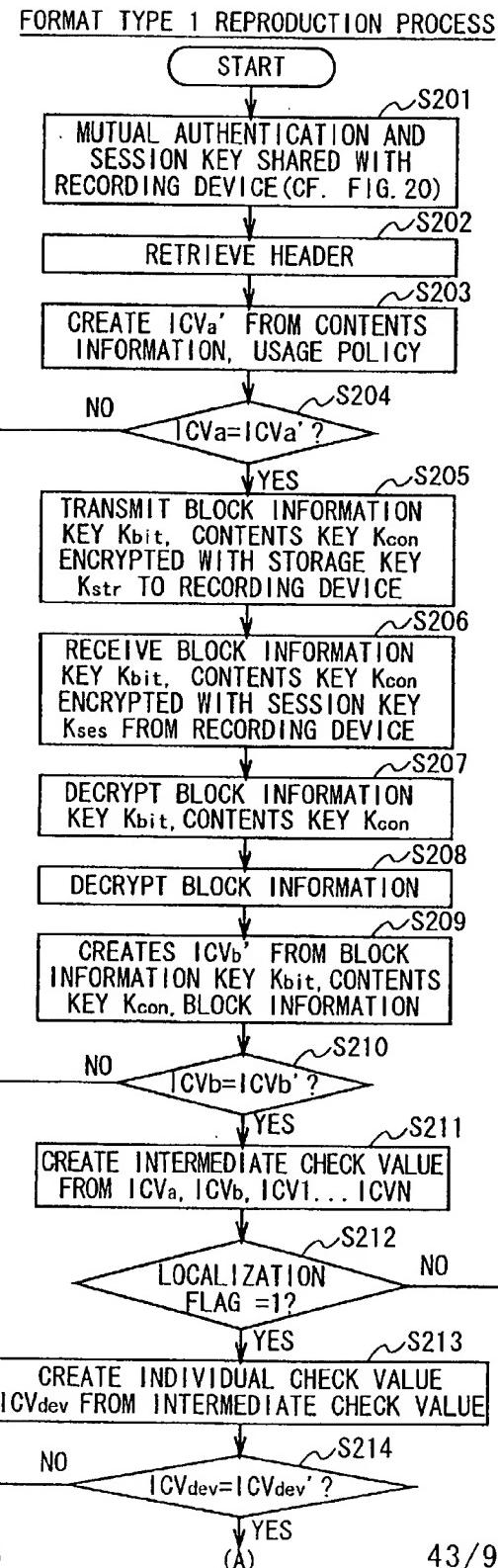


FIG. 43

09/937410

FOURTY-EIGHT SEVEN

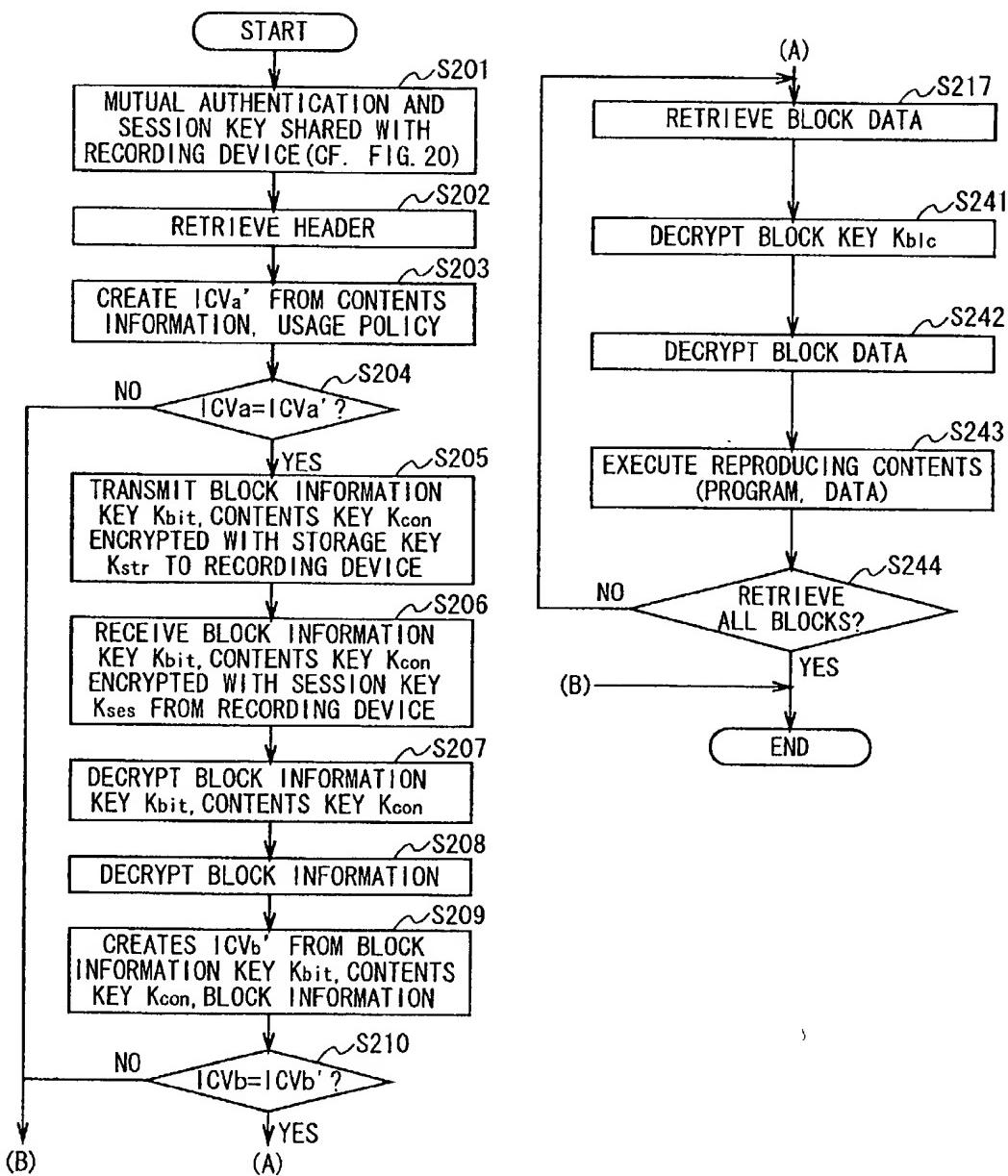


FIG. 44

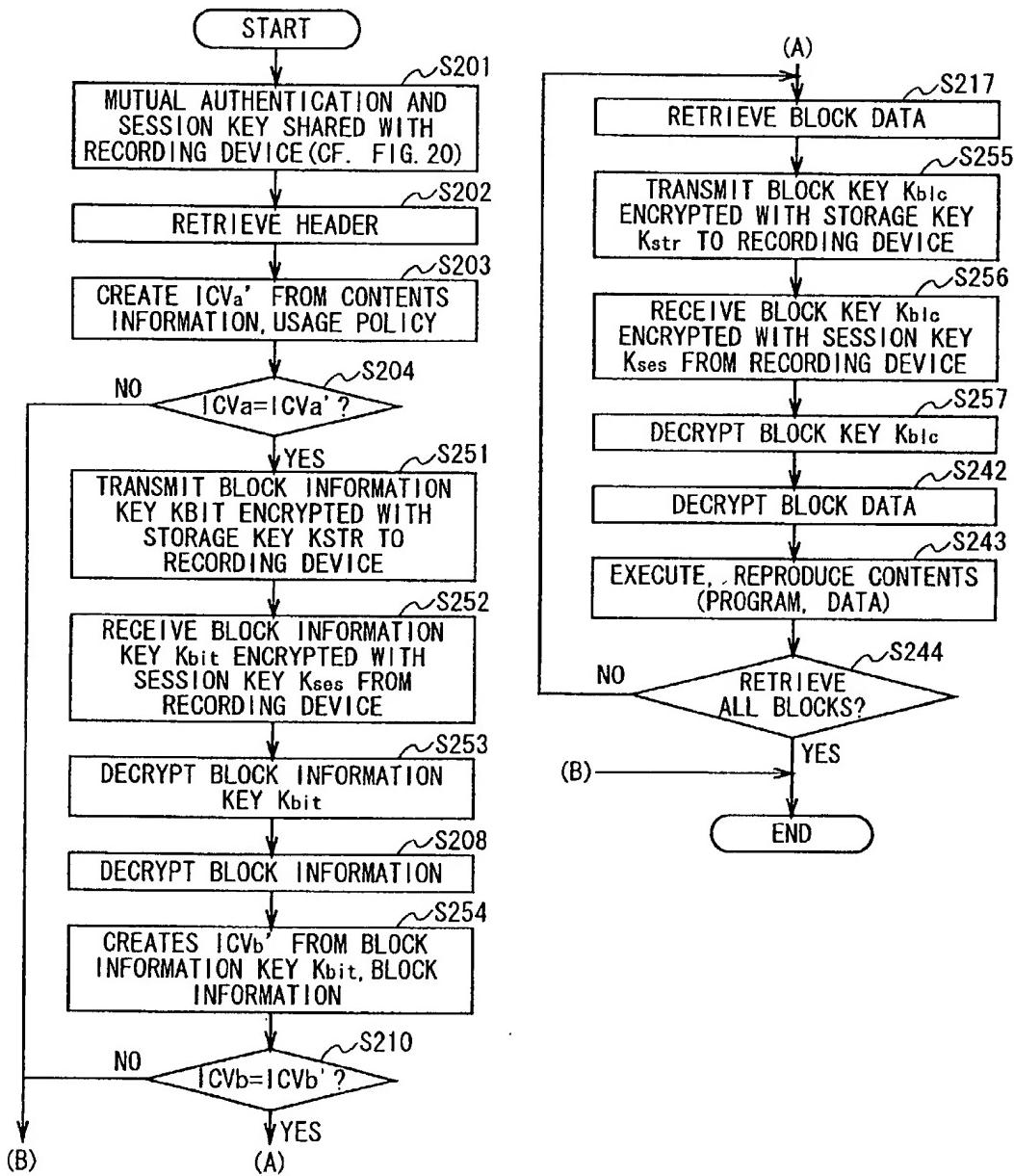
FORMAT TYPE 3 REPRODUCTION PROCESS

FIG. 45

DATA FOR VERIFICATION

09/937410

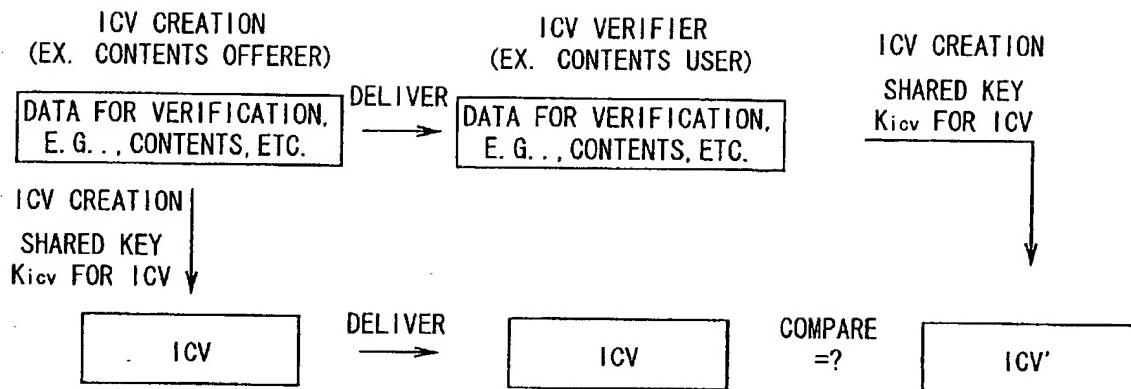


FIG. 46

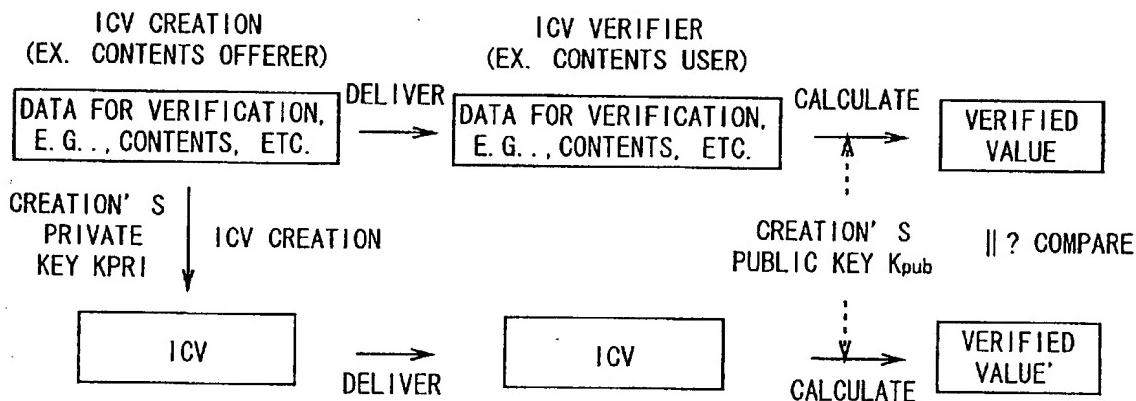


FIG. 47

09/937410

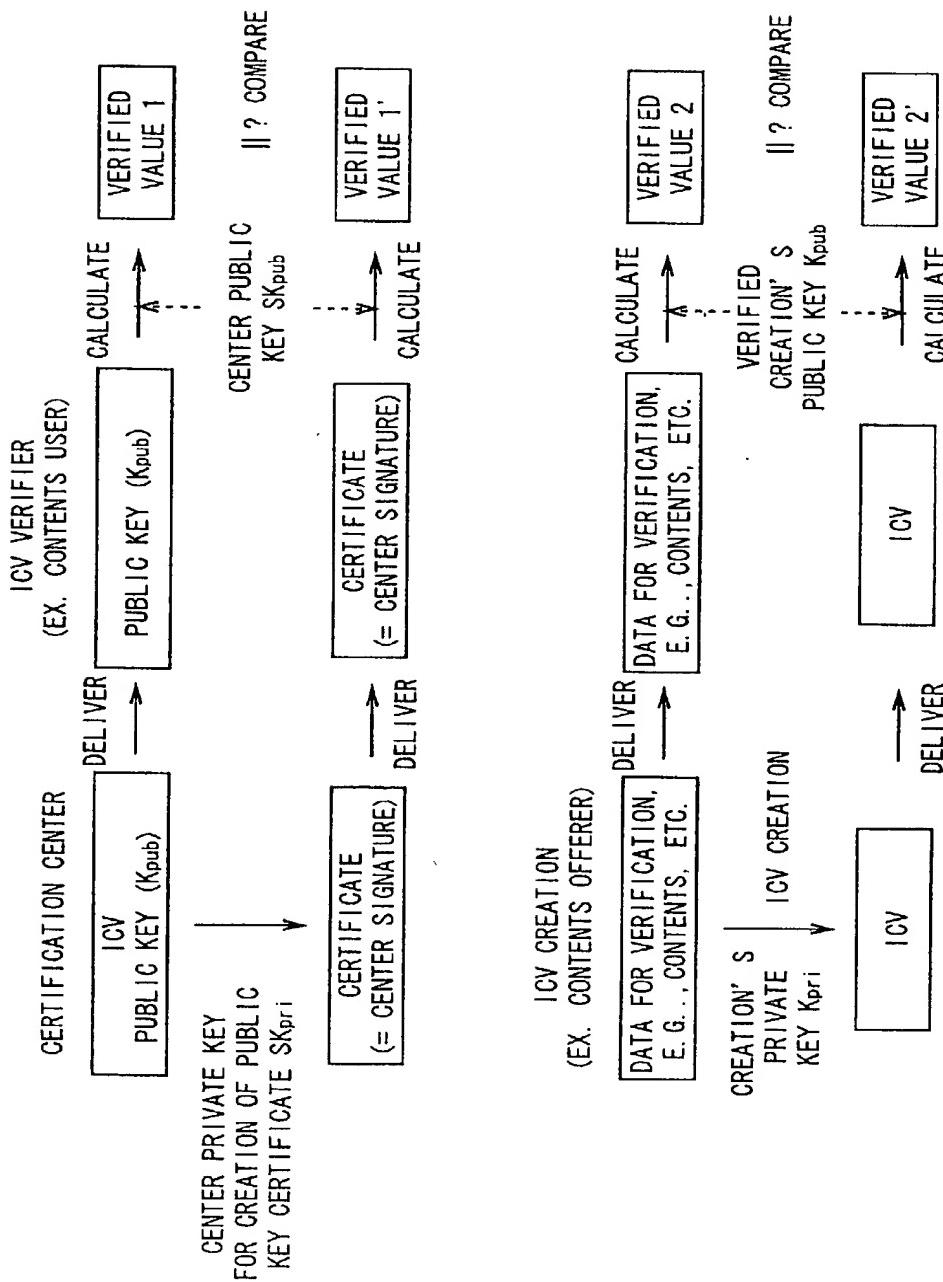


FIG. 48

TO ZONE - DATA EXCH

09/937410

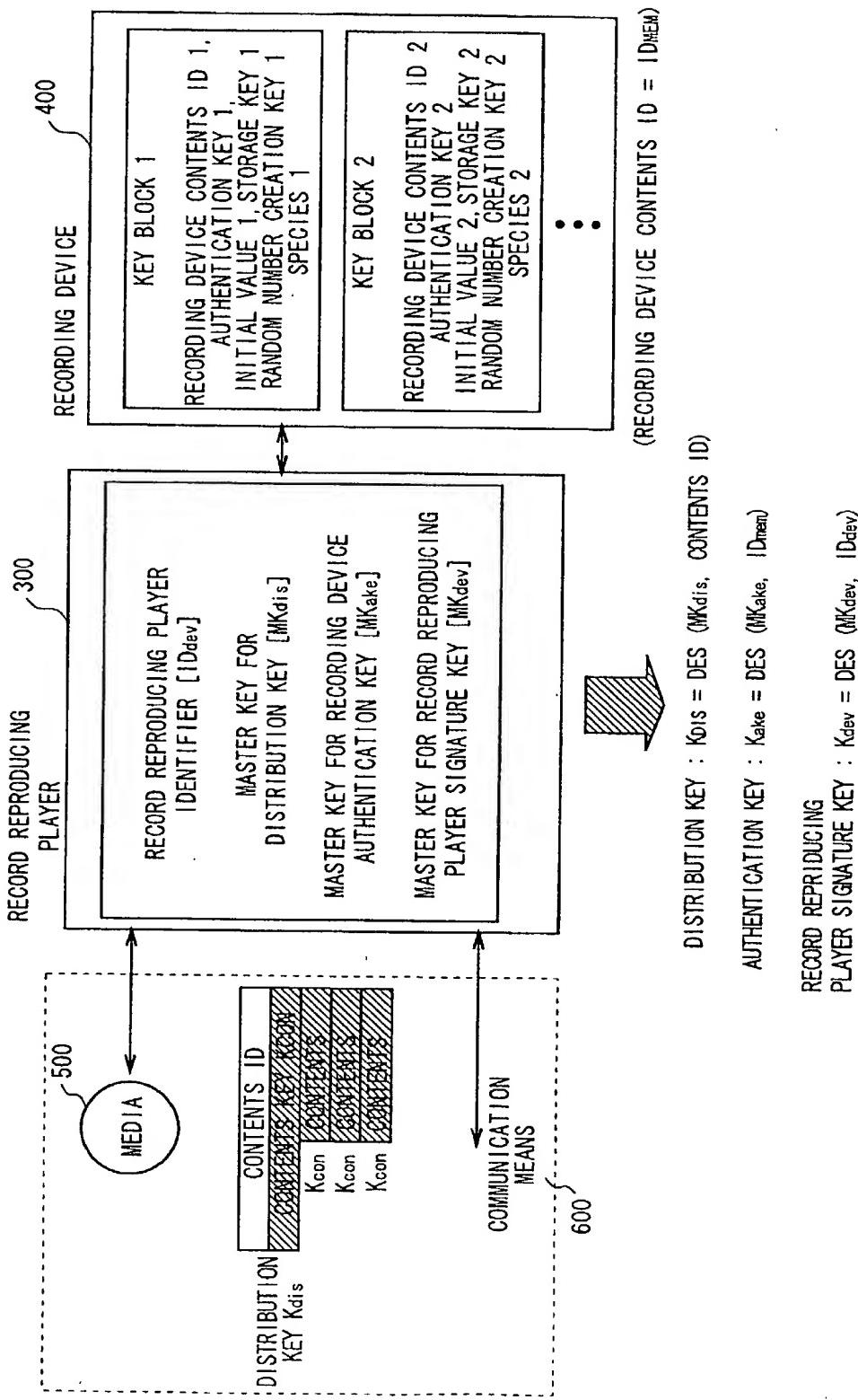
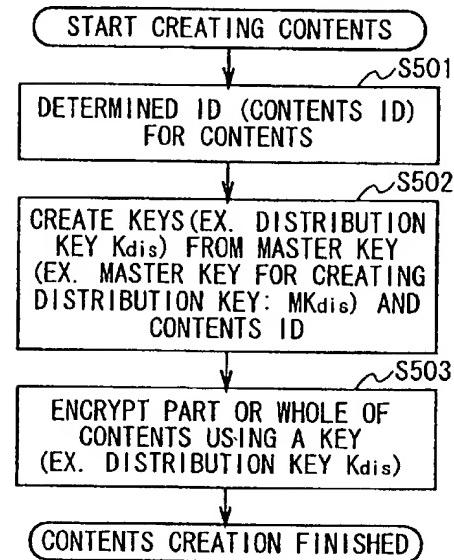


FIG. 49

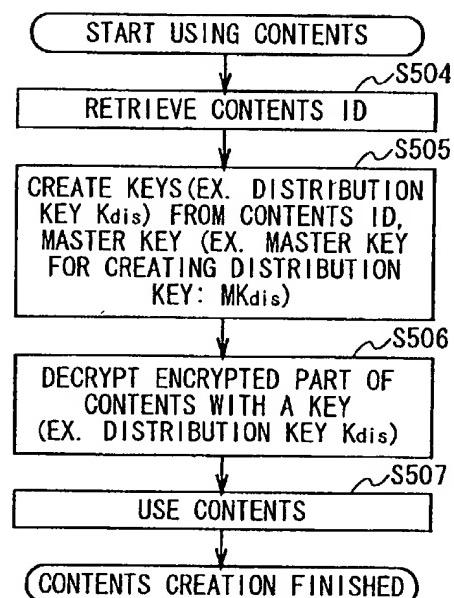
METHOD TO CREATE INDIVIDUAL KEYS FROM MASTER KEY-(1)

[BASIC FLOW]

CONTENTS CREATION OR ADMINISTRATOR

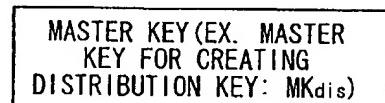


USER DEVICE



[KEY POSSESSION COMPOSITION]

CONTENTS CREATION OR ADMINISTRATOR



USER DEVICE

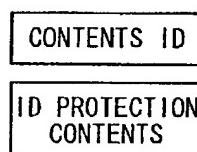


FIG. 50

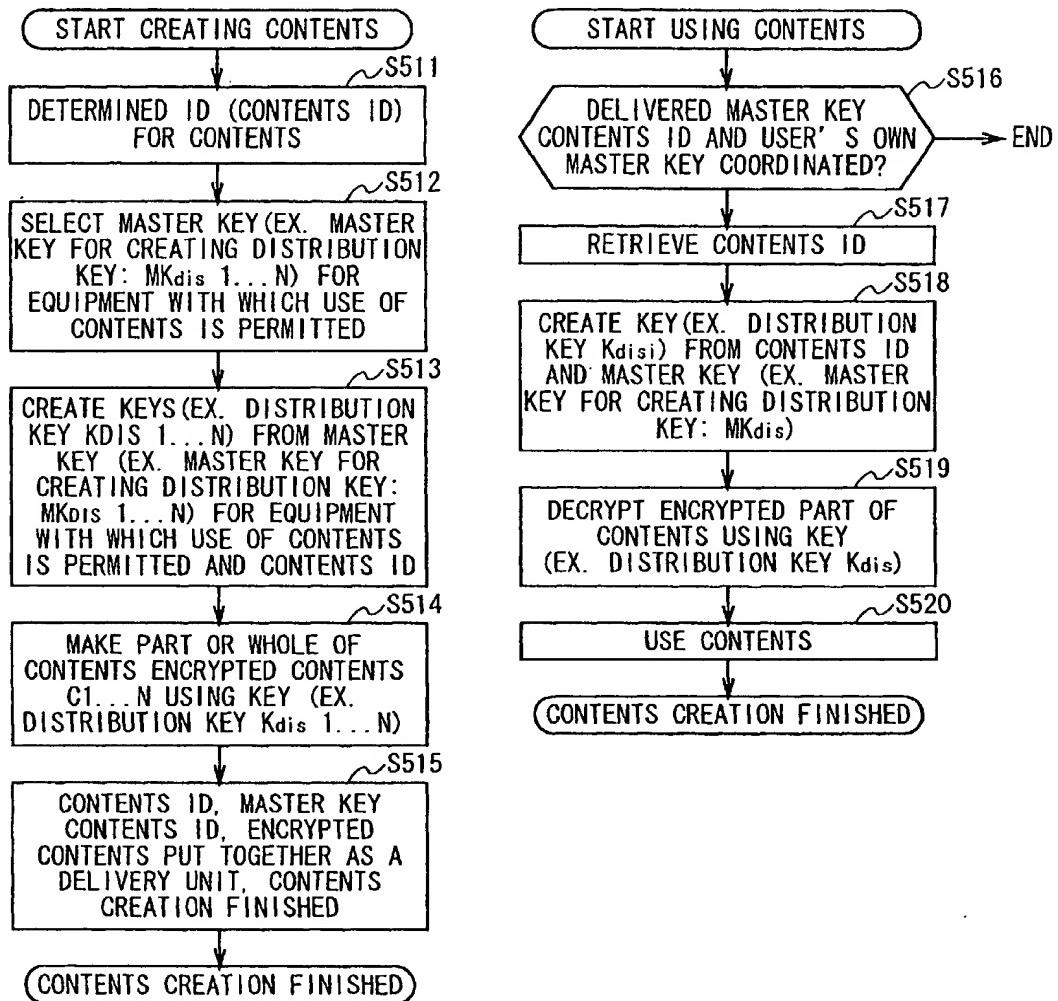
09/937410

METHOD TO CREATE INDIVIDUAL KEYS FROM MASTER KEY-(2)

[BASIC FLOW]

CONTENTS CREATION OR ADMINISTRATOR

USER DEVICE



[KEY POSSESSION COMPOSITION]

CONTENTS CREATION OR ADMINISTRATOR

USER DEVICE

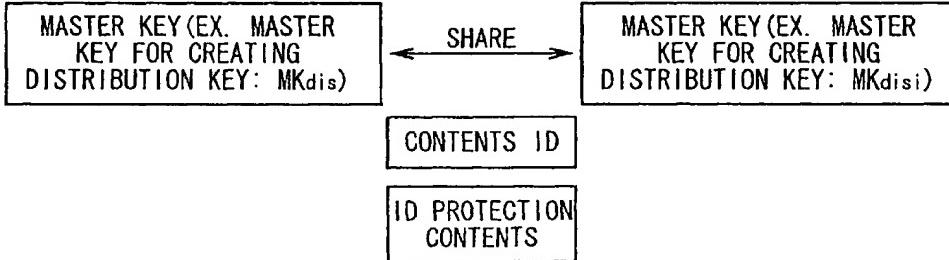
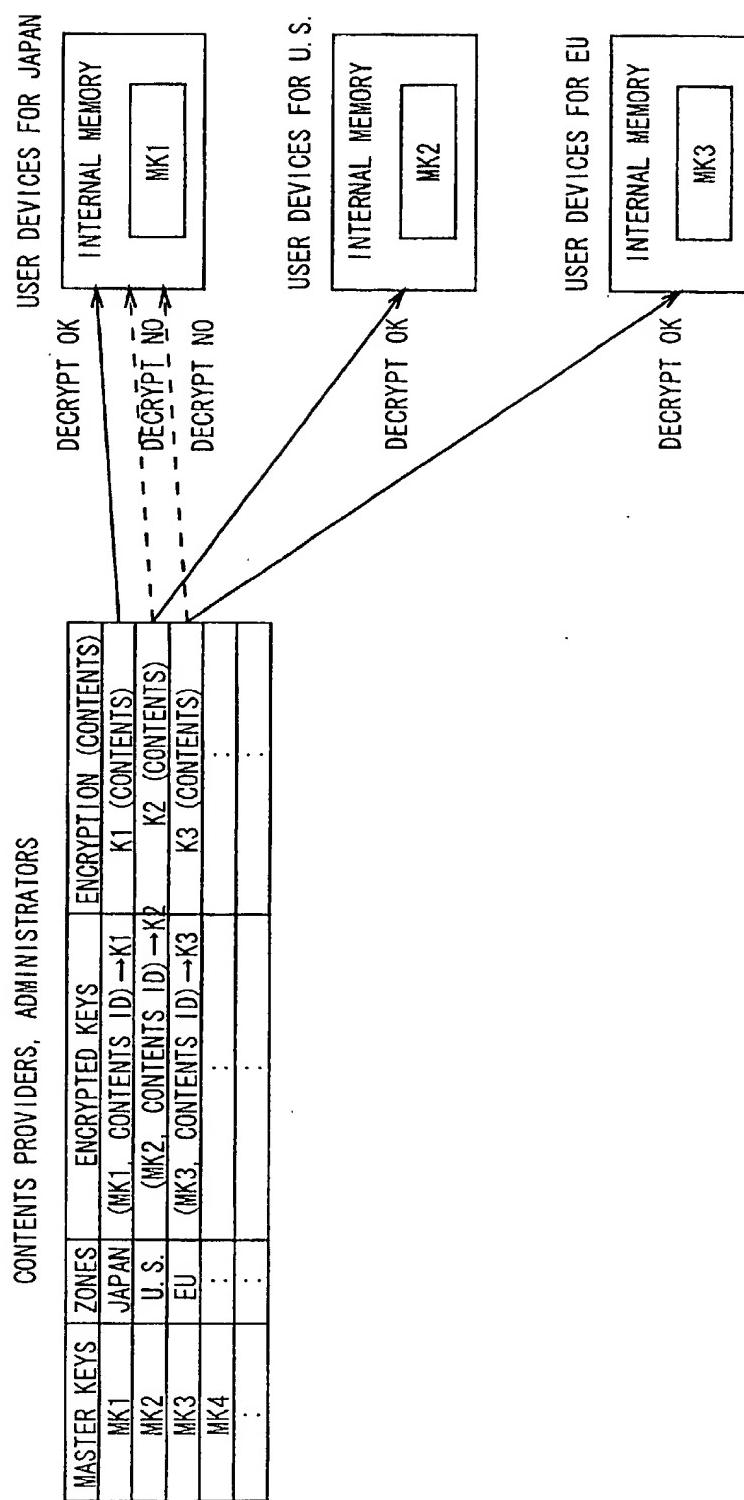


FIG. 51

TOP SECRET//COMINT

09/937410

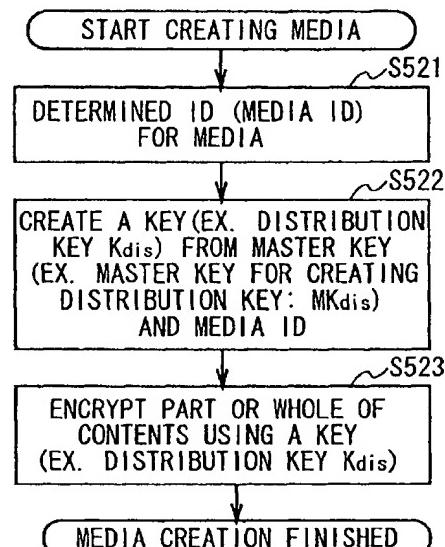


09/937410

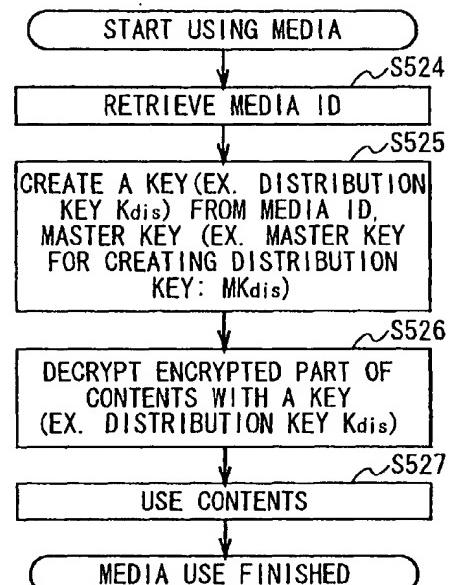
METHOD TO CREATE INDIVIDUAL KEYS FROM MASTER KEY- (3)

[BASIC FLOW]

MEDIA CREATION OR ADMINISTRATOR



USER DEVICE



[KEY POSSESSION COMPOSITION]

MEDIA CREATION OR ADMINISTRATOR

MASTER KEY (EX. MASTER KEY FOR CREATING DISTRIBUTION KEY: MKdis)

USER DEVICE

MASTER KEY (EX. MASTER KEY FOR CREATING DISTRIBUTION KEY: MKdis)

SHARE

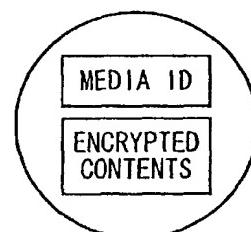
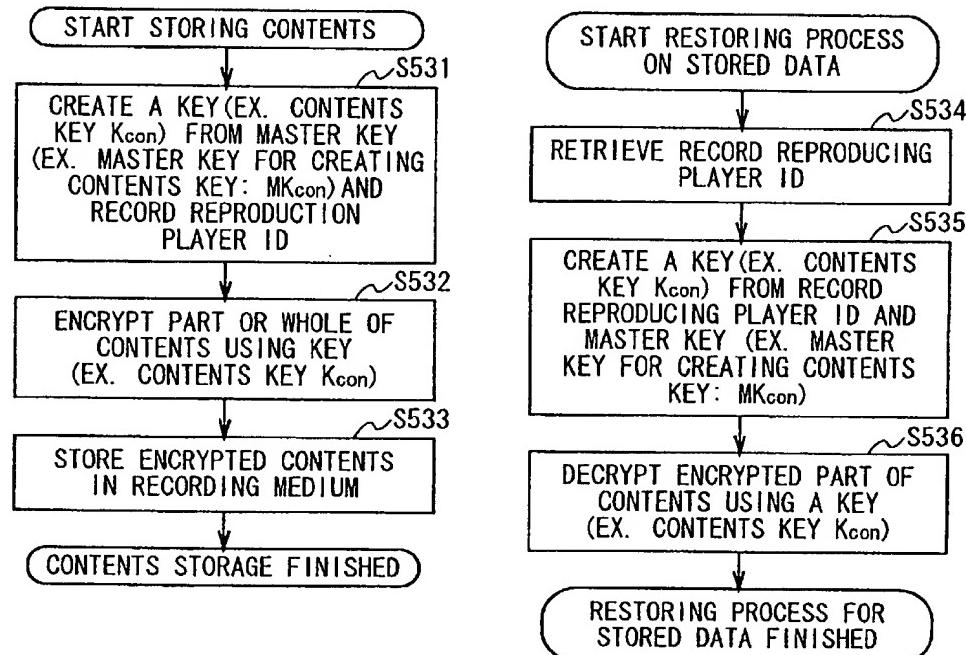


FIG. 53

METHOD TO CREATE INDIVIDUAL KEYS FROM MASTER KEY - (4)
 [BASIC FLOW]

RECORD REPRODUCING PLAYER USER

SYSTEM ADMINISTRATOR



[KEY POSSESSION COMPOSITION]

RECORD REPRODUCING PLAYER USER

SYSTEM ADMINISTRATOR

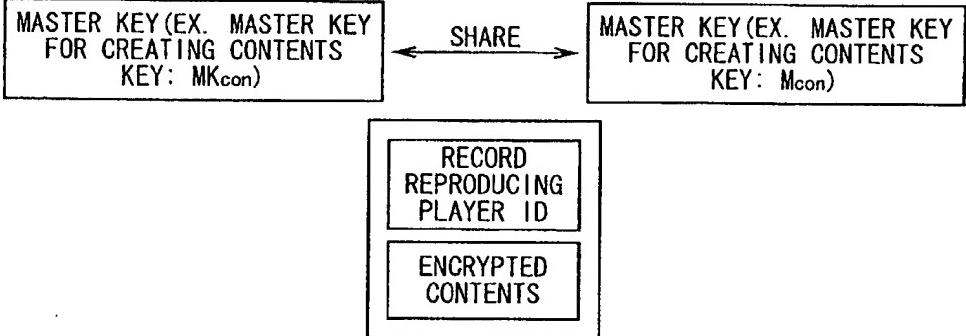
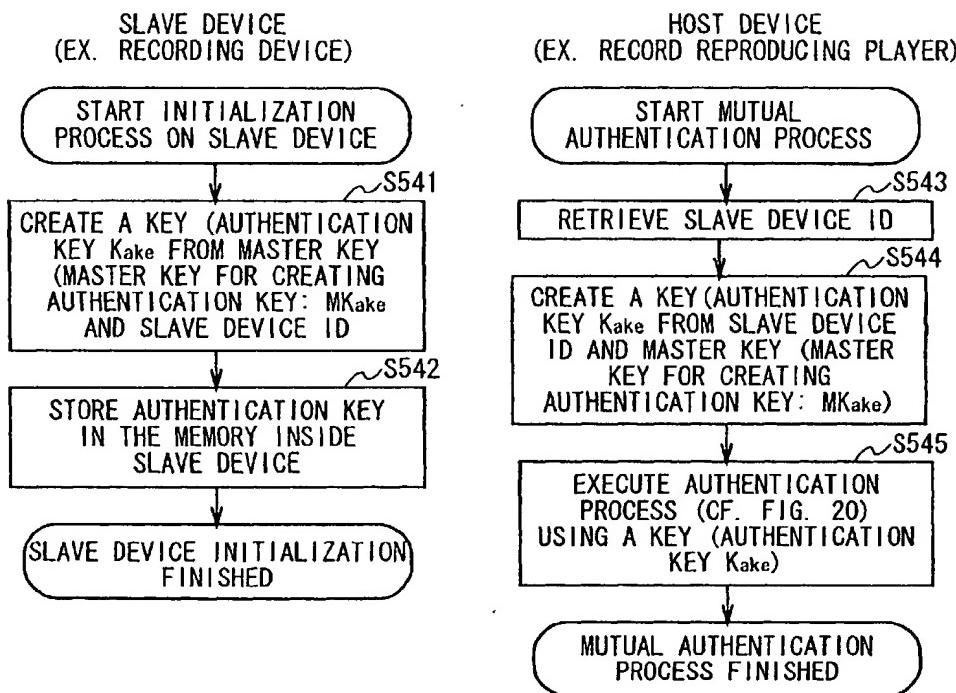


FIG. 54

METHOD TO CREATE INDIVIDUAL KEYS FROM MASTER KEY- (5)
 [BASIC FLOW]

FOURTEEN FIGURES



[KEY POSSESSION COMPOSITION]

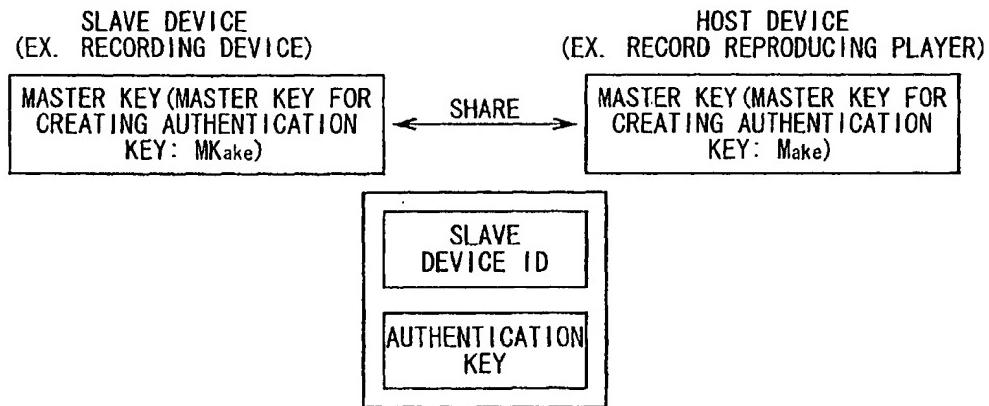


FIG. 55

TOP SECRET - OFFICE OF THE CHIEF OF STAFF

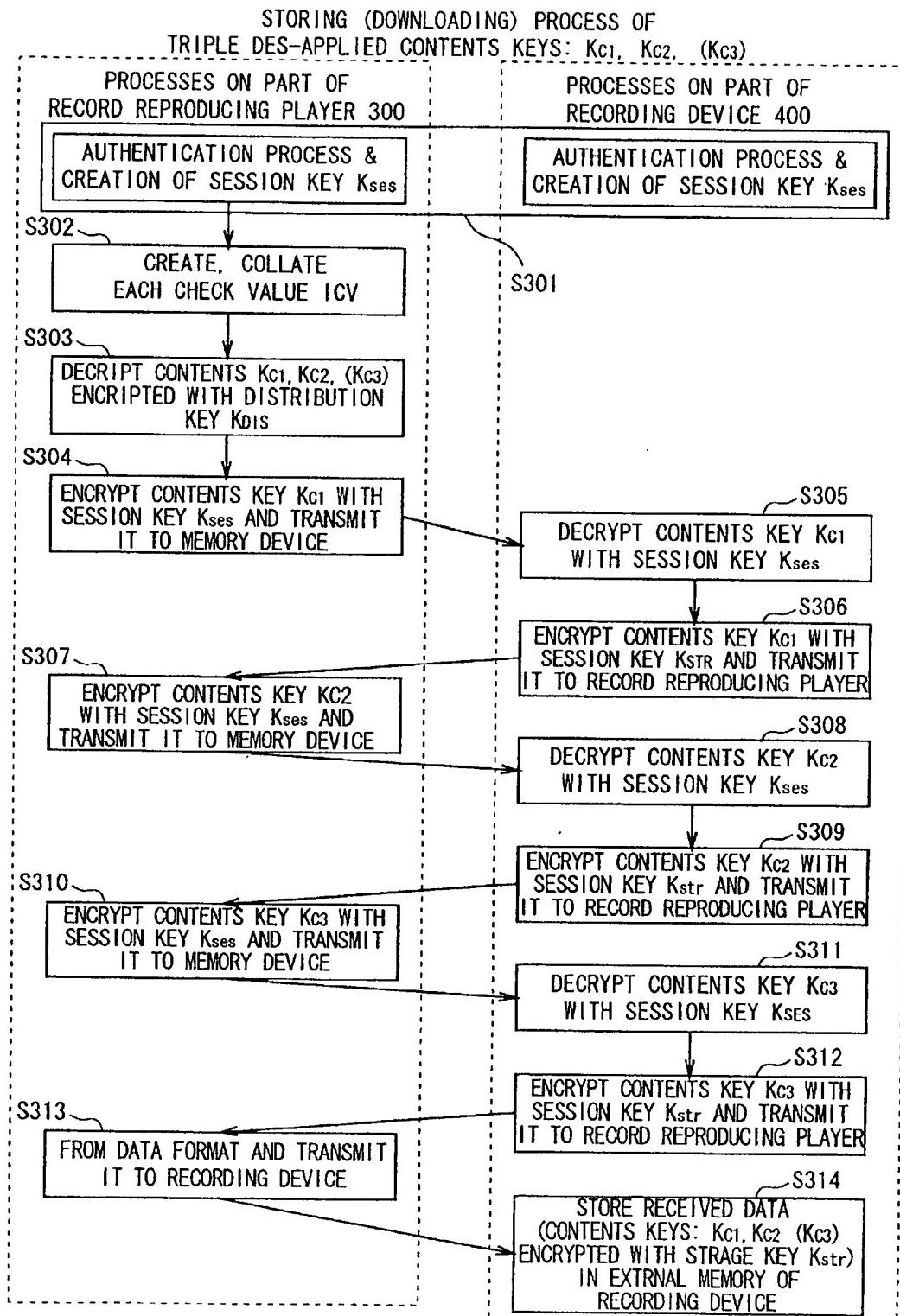


FIG. 56

FOOTER:0914660

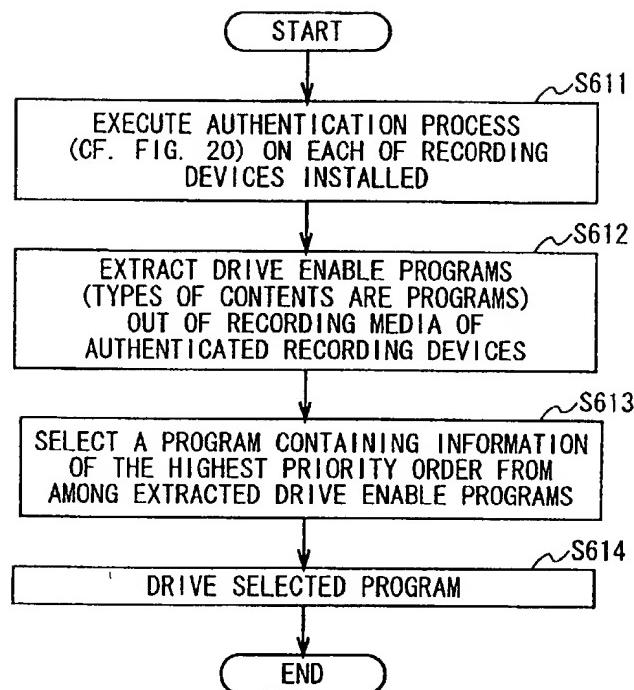


FIG. 57

TOP SECRET//COMINT

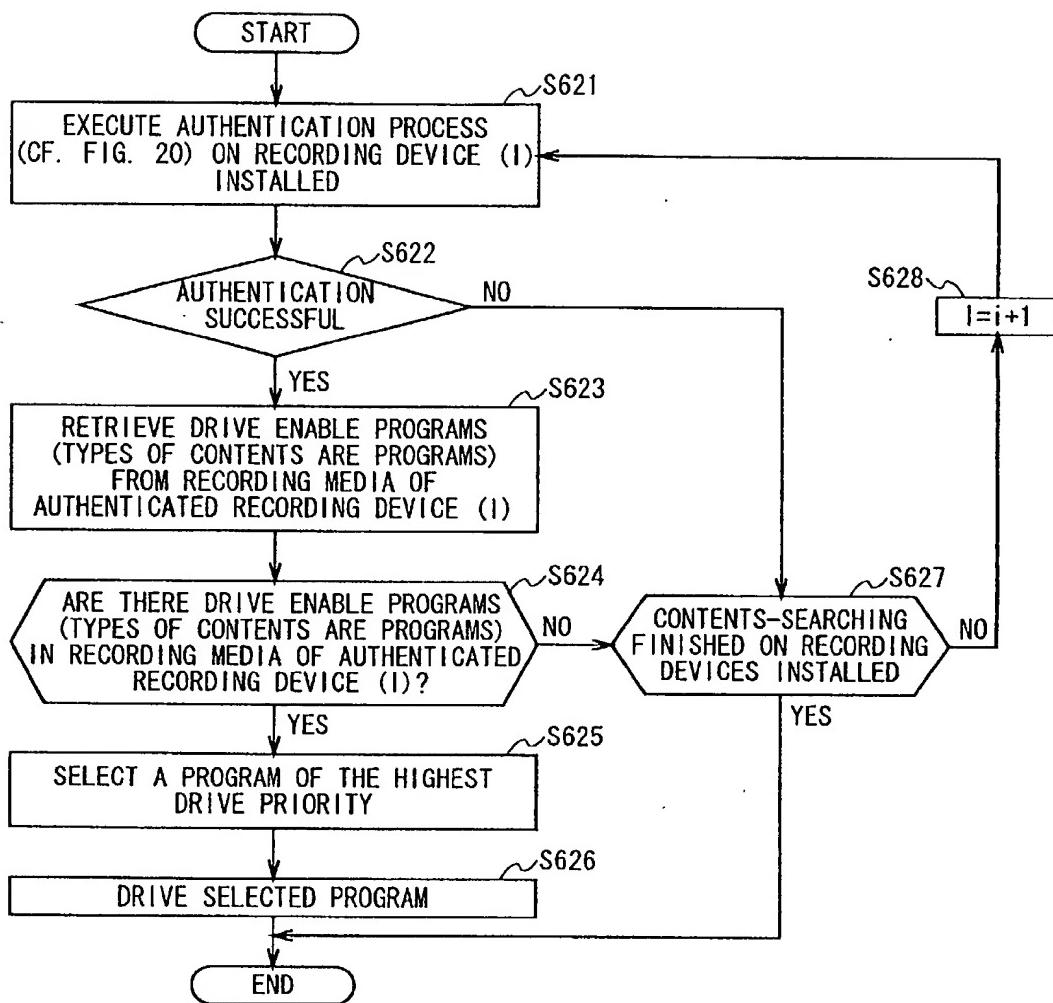


FIG. 58

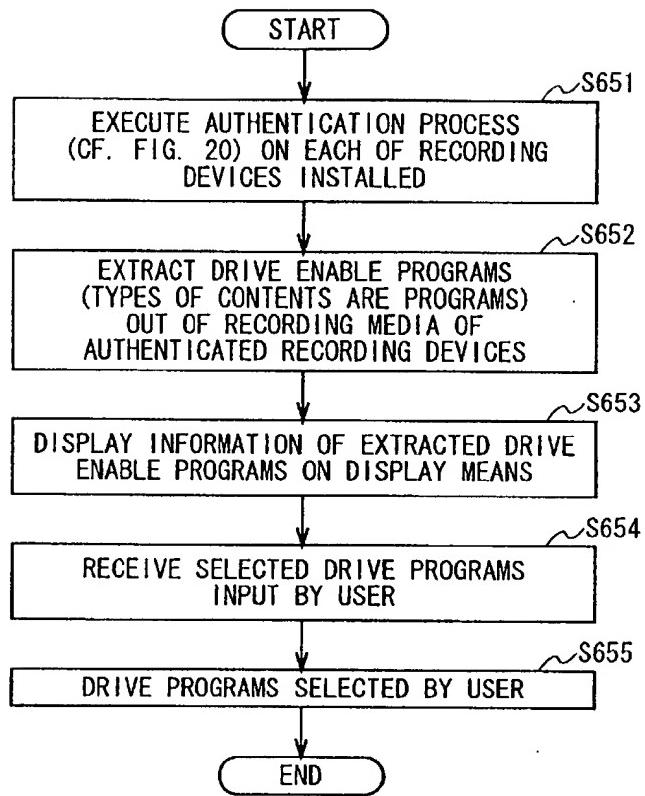


FIG. 59

09/937410

TELETYPE OUTLINE DRAWING

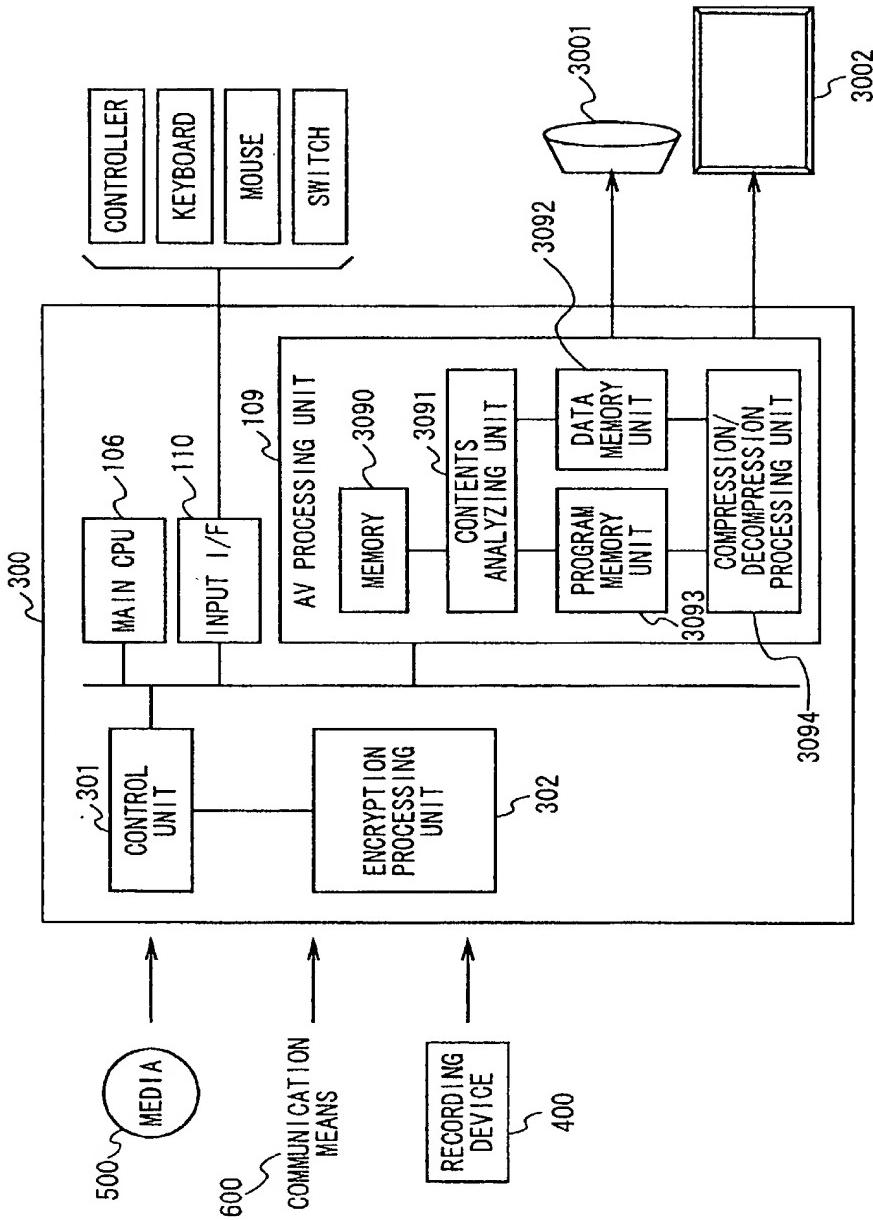


FIG. 60

09/937410

EXAMPLE OF CONTENTS COMPOSITION (1)

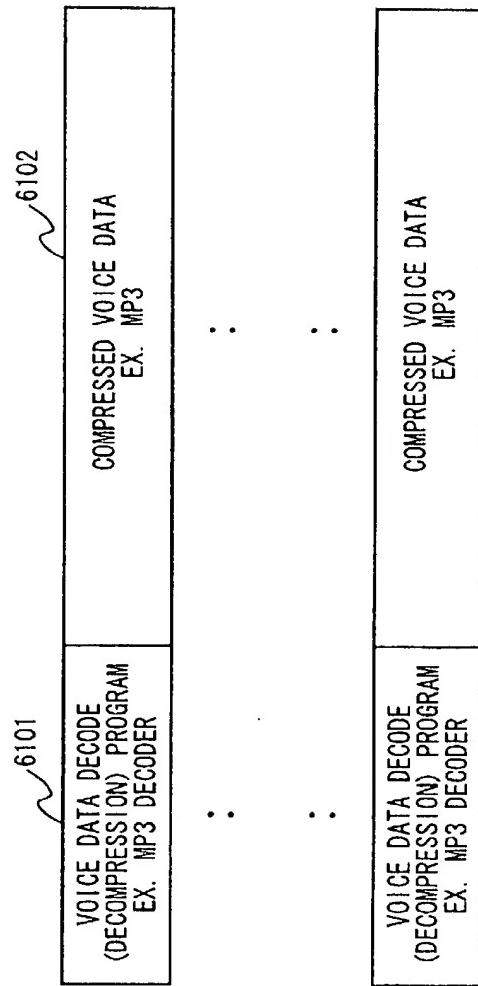


FIG. 61

09/937410

TOP SECRET//COMINT

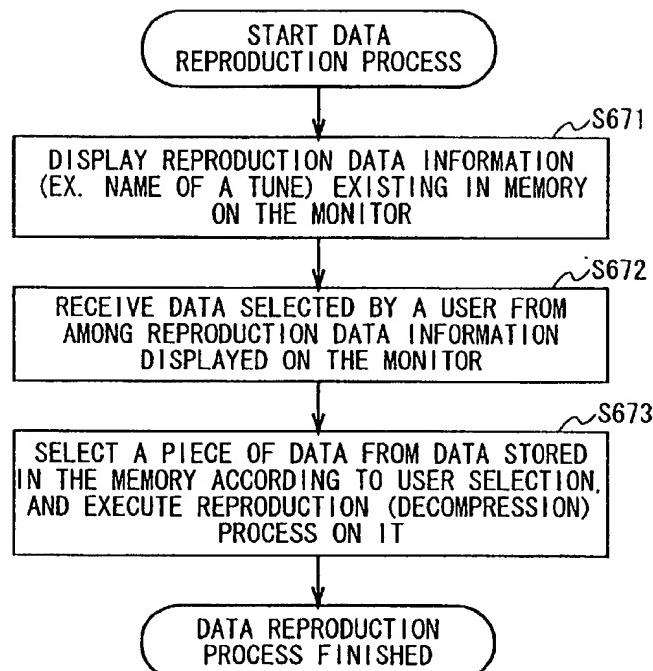


FIG. 62

09/937410

TIJDSFEST = OTTHXEESGO

EXAMPLE OF CONTENTS COMPOSITION (2)

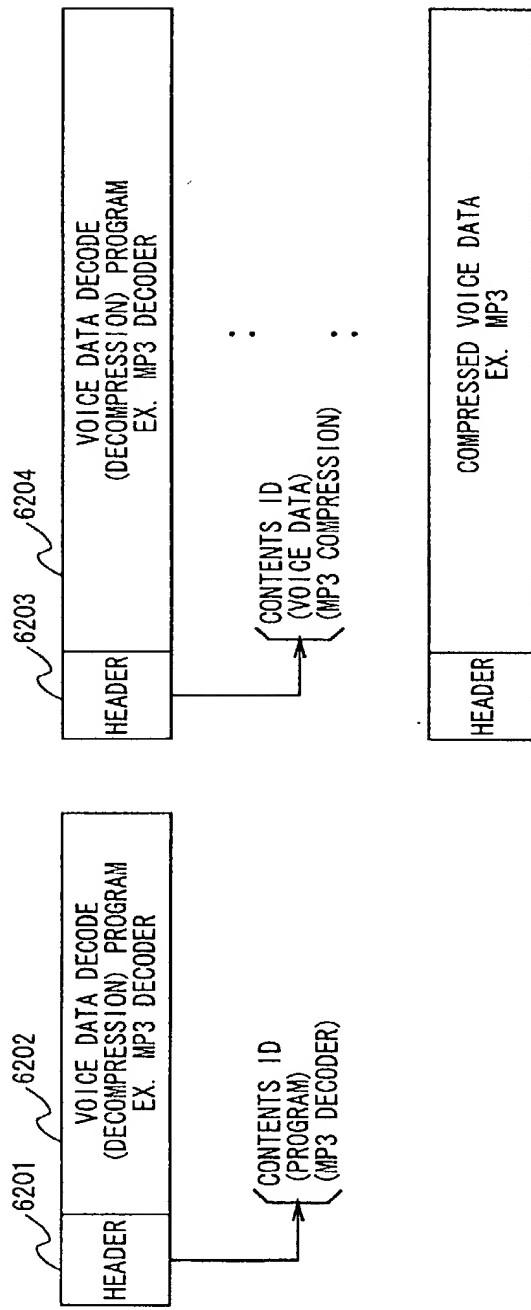


FIG. 63

ROCKET-OT412E650

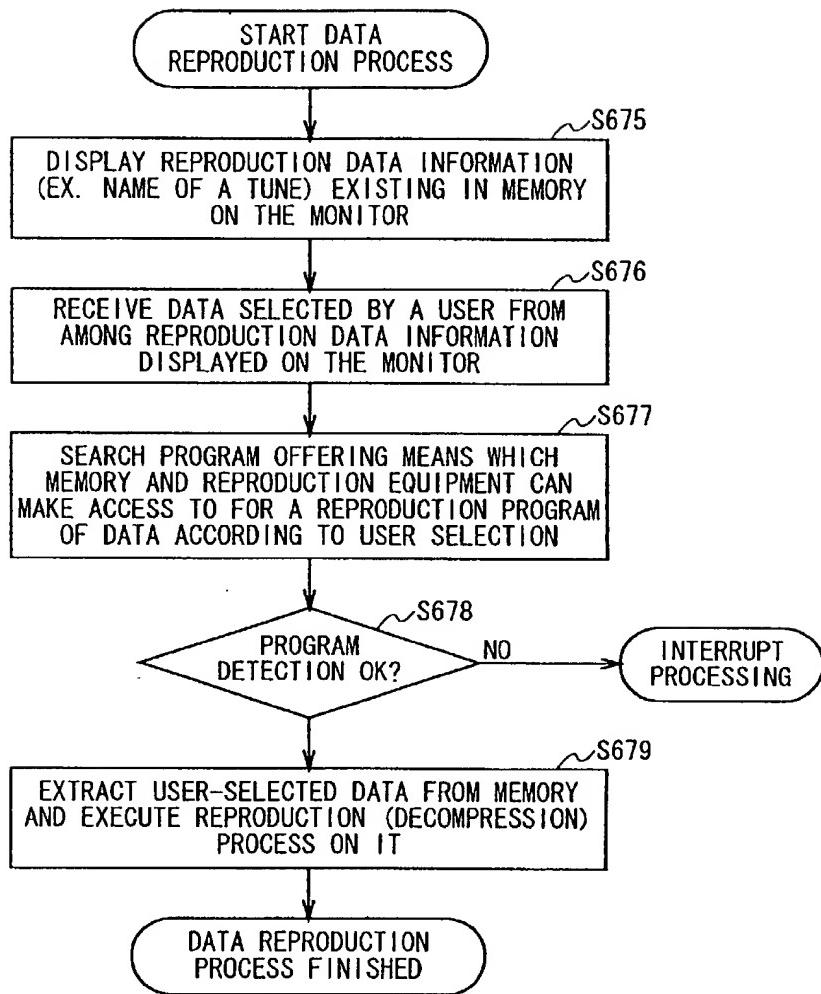


FIG. 64

09/937410

TRAFFIC DATA FILE

EXAMPLE OF CONTENTS COMPOSITION (3)

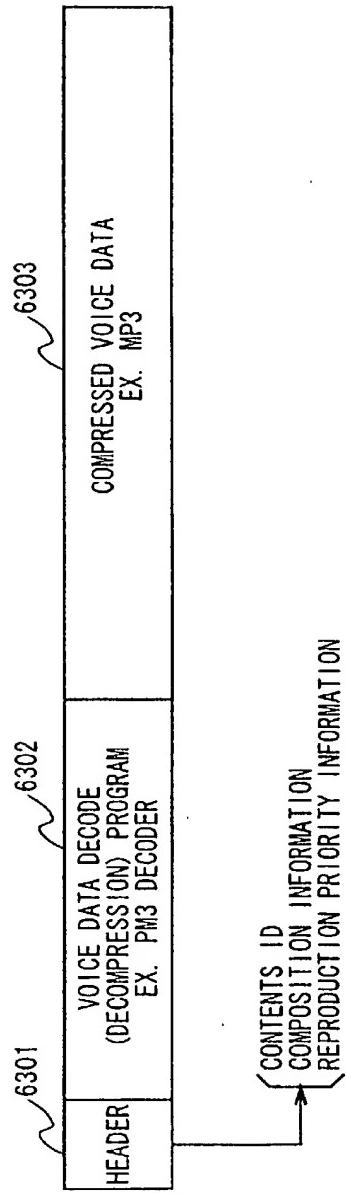


FIG. 65

09/937410

TOP SECRET//COMINT

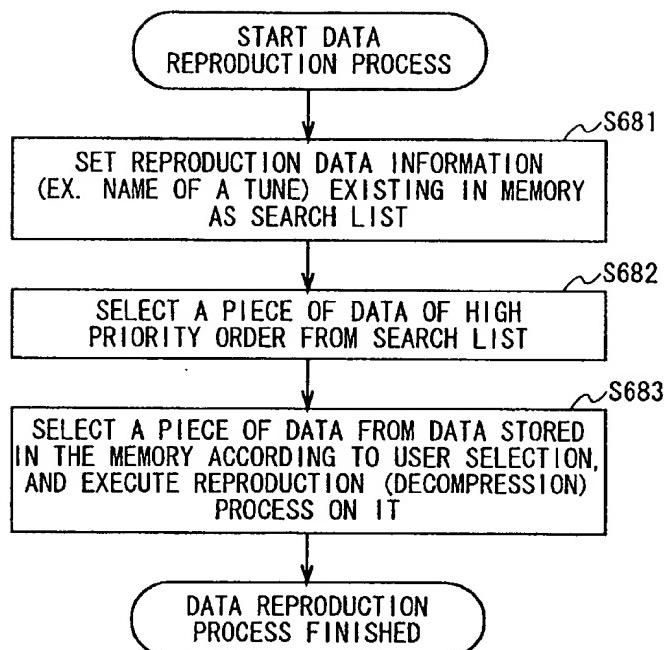


FIG. 66

EXAMPLE OF CONTENTS COMPOSITION (4)

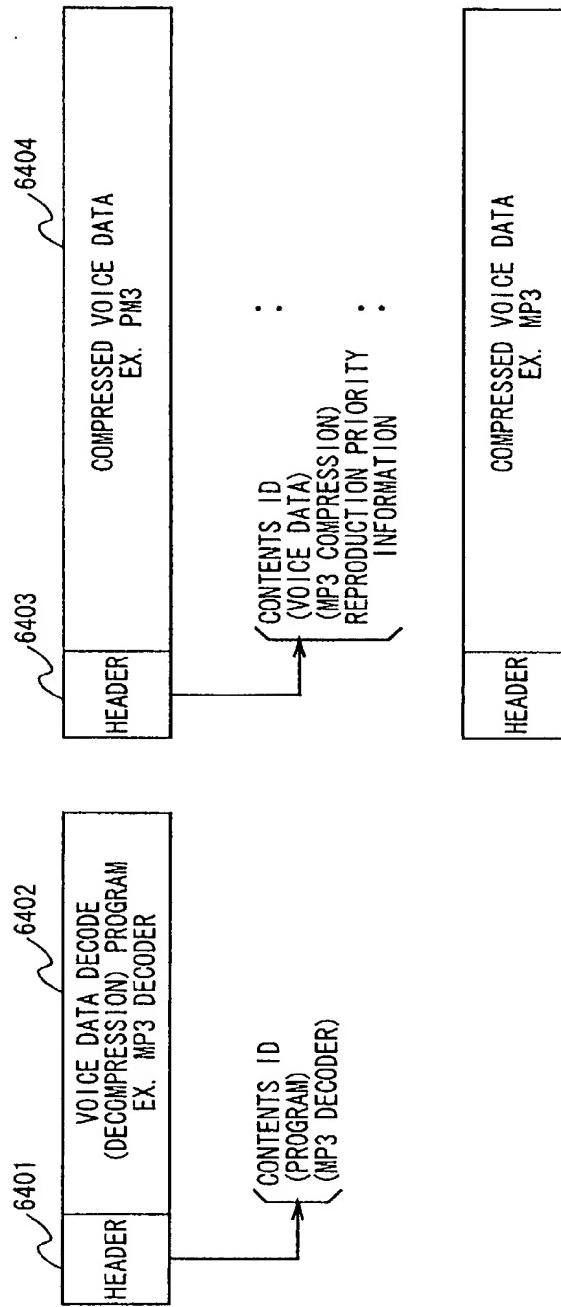


FIG. 67

TOP SECRET//DECODED

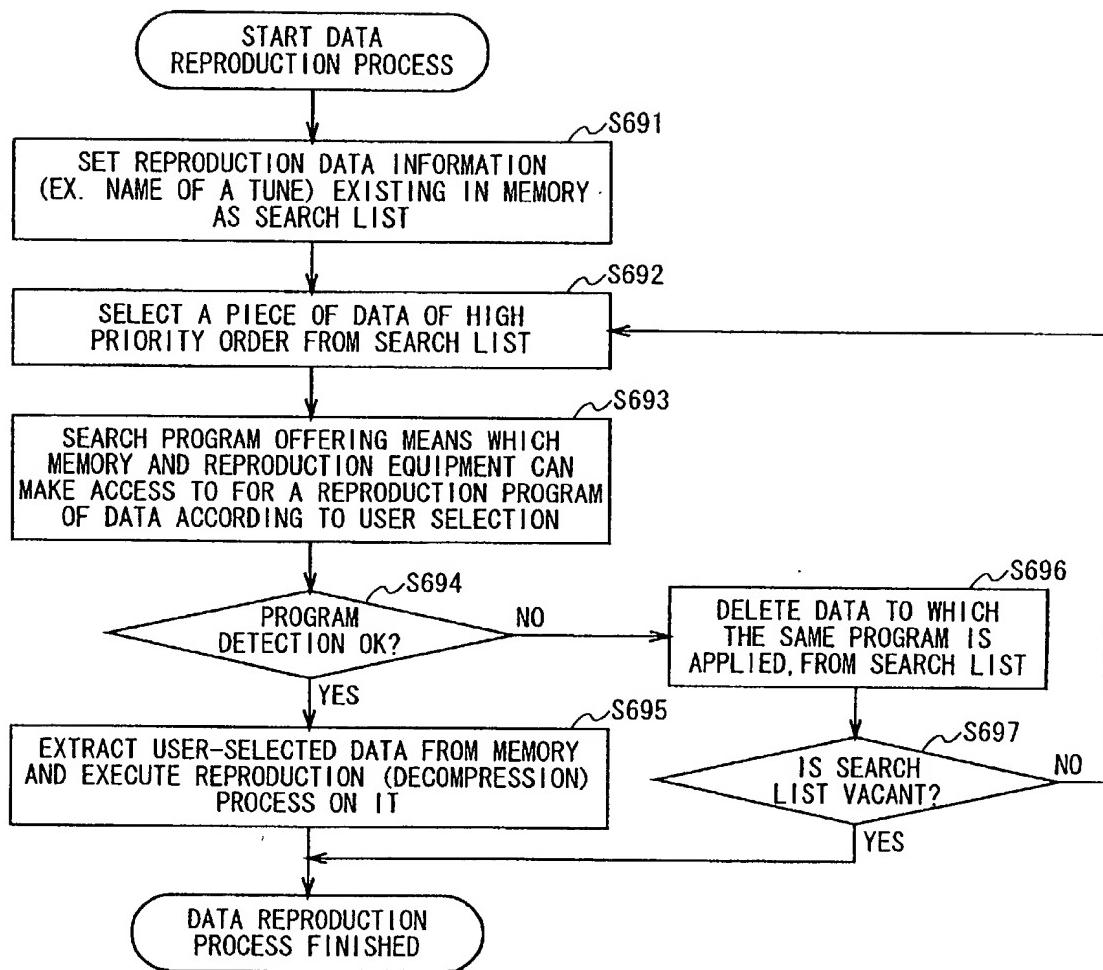
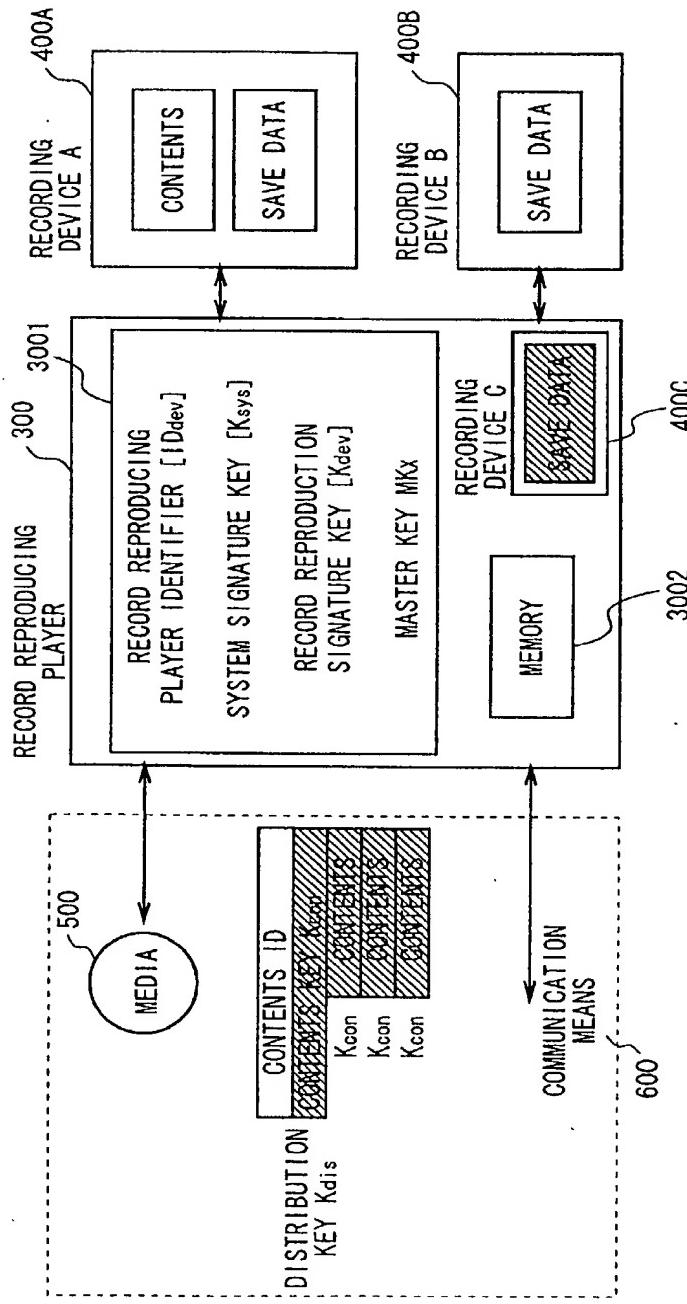


FIG. 68



SAVE DATA ENCRYPTION KEY: K_{sav}=K_{con}
 SAVE DATA ENCRYPTION KEY: K_{sav}=K_{dev}
 SAVE DATA ENCRYPTION KEY: K_{sav}=CONTENTS ID, (MK_x, CONTENTS ID)
 SAVE DATA ENCRYPTION KEY: K_{sav}=RECORD REPRODUCING PLAYER ID (ID_{dev})
 SAVE DATA ENCRYPTION KEY: K_{sav}= (K_{con}, K_{dev}) or DES (MK_x, K_{con}, K_{dev})
 SAVE DATA ENCRYPTION KEY: K_{sav}= (CONTENT ID, K_{dev}) or DES (MK_x, CONTENT ID, K_{dev})
 SAVE DATA ENCRYPTION KEY: K_{sav}= (KCON RECORD REPRODUCING PLAYER ID) or DES (MK_x, K_{con}, RECORD REPRODUCING PLAYER ID) or DES (CONTENTS ID, RECORD REPRODUCING PLAYER ID) or DES (MK_x, CONTENTS ID, RECORD REPRODUCING PLAYER ID)
 SAVE DATA ENCRYPTION KEY: K_{sav}=PASSWORD OR DES (MK_x, PASSWORD) ETC.

09/937410

(1) EXAMPLE OF SAVE DATA STORAGE PROCESS USING CONTENTS INDIVIDUAL KEY, OR SYSTEM SHARED KEY

TOP SECRET - OFFICE 650

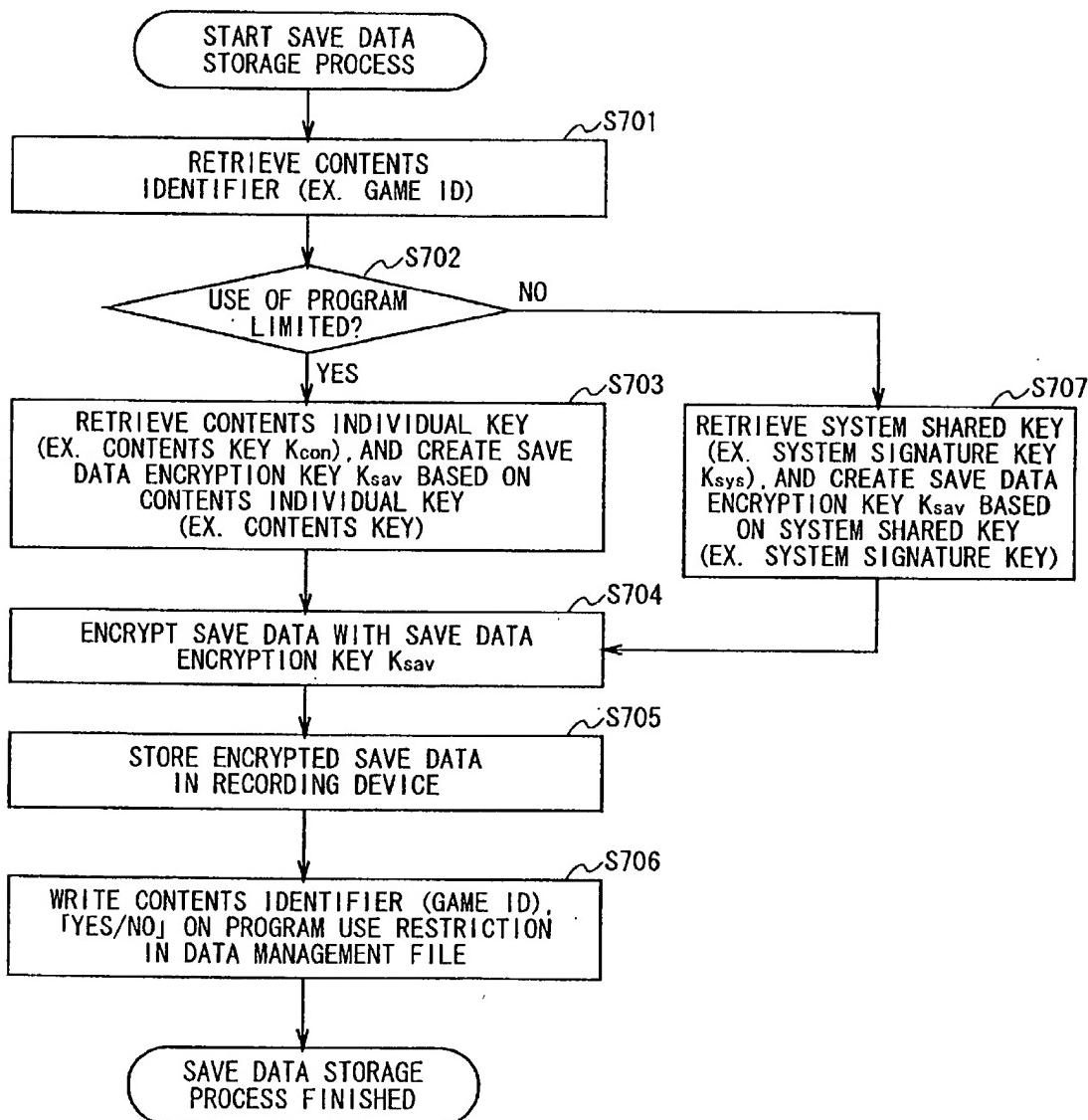


FIG. 70

TECHNICAL OFFICE EDITION

09/937410

DATA MANAGEMENT FILE (1)

DATA NO.	CONTENTS IDENTIFIER (GAME ID)	RECORD REPRODUCING PLAYER IDENTIFIER (ID _{dev})	PROGRAM USE RESTRICTION
1	12345678...	56789012...	YES
2	ABCDEF12...	09876543...	YES
3	12245678...	58834762...	NO
:	:	:	:

FIG. 71

70/93

09/937410

(2) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING CONTENTS INDIVIDUAL KEY, OR SYSTEM SHARED KEY

TOP SECRET//FOUO//EYES

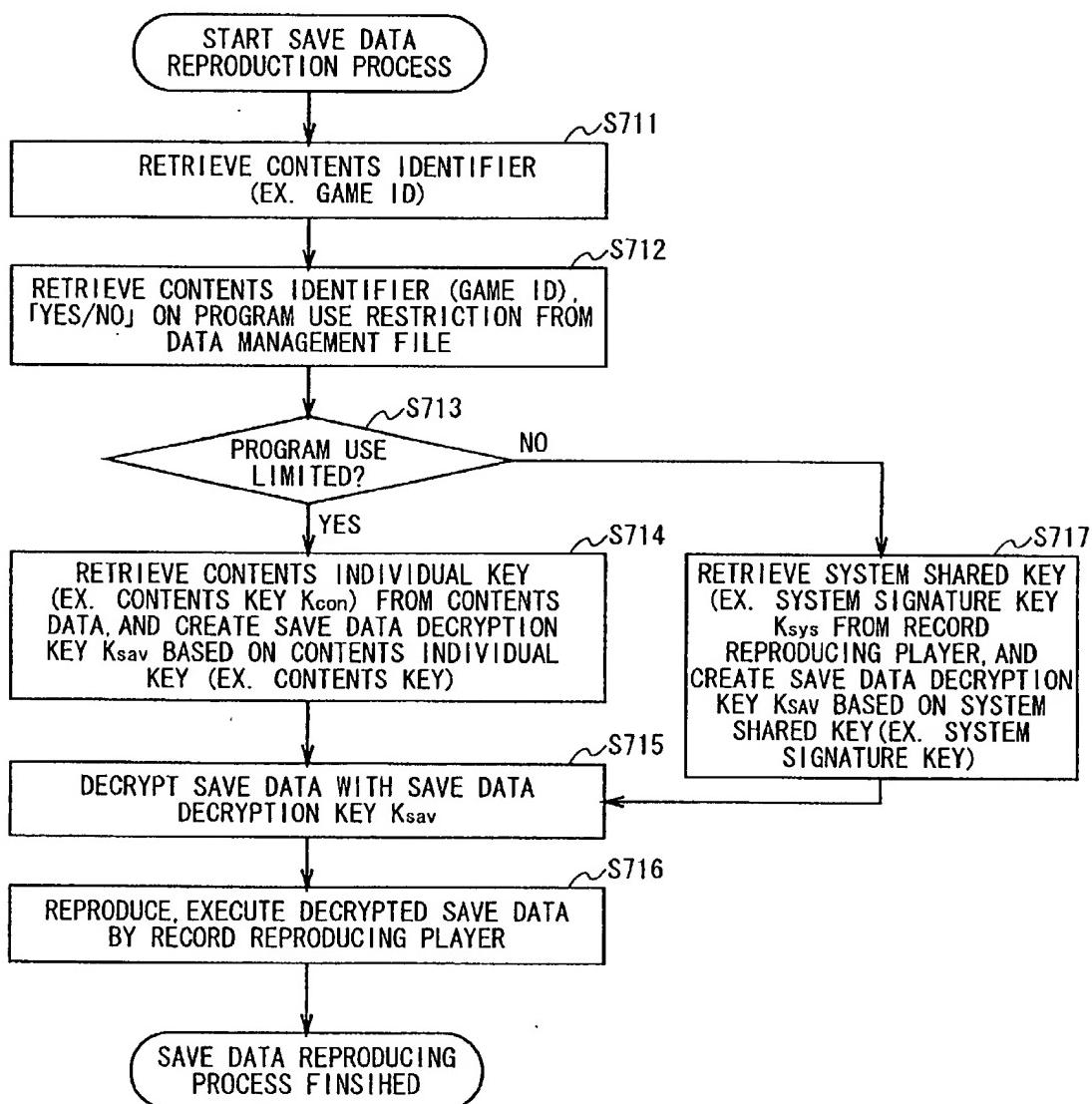


FIG. 72

(3) EXAMPLE OF SAVE DATA STORAGE PROCESS USING CONTENTS ID, OR SYSTEM SHARED KEY

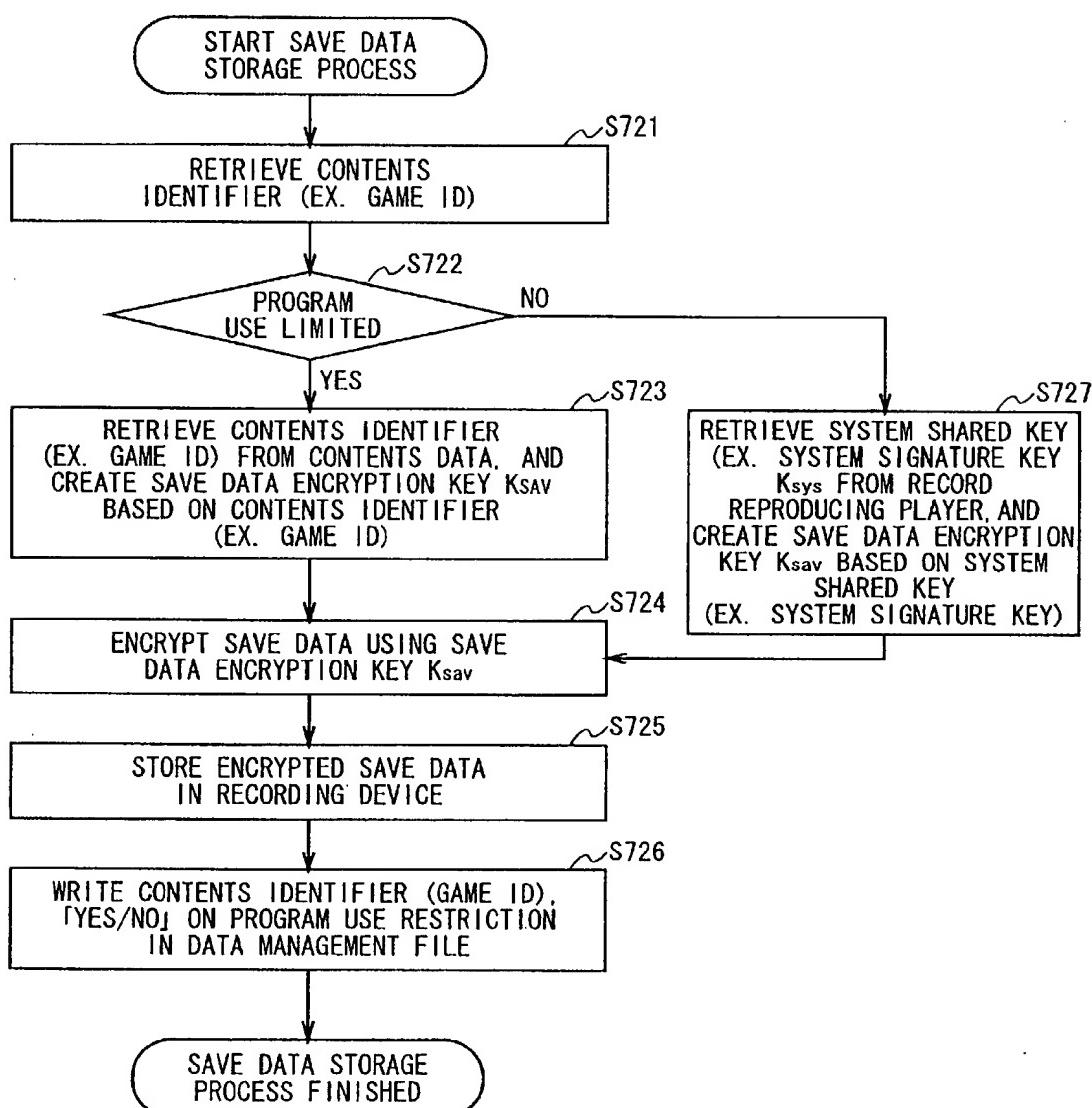


FIG. 73

09/937410

(4) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING
CONTENTS ID, OR SYSTEM SHARED KEY

TOP SECRET//~~REF ID: A66660~~

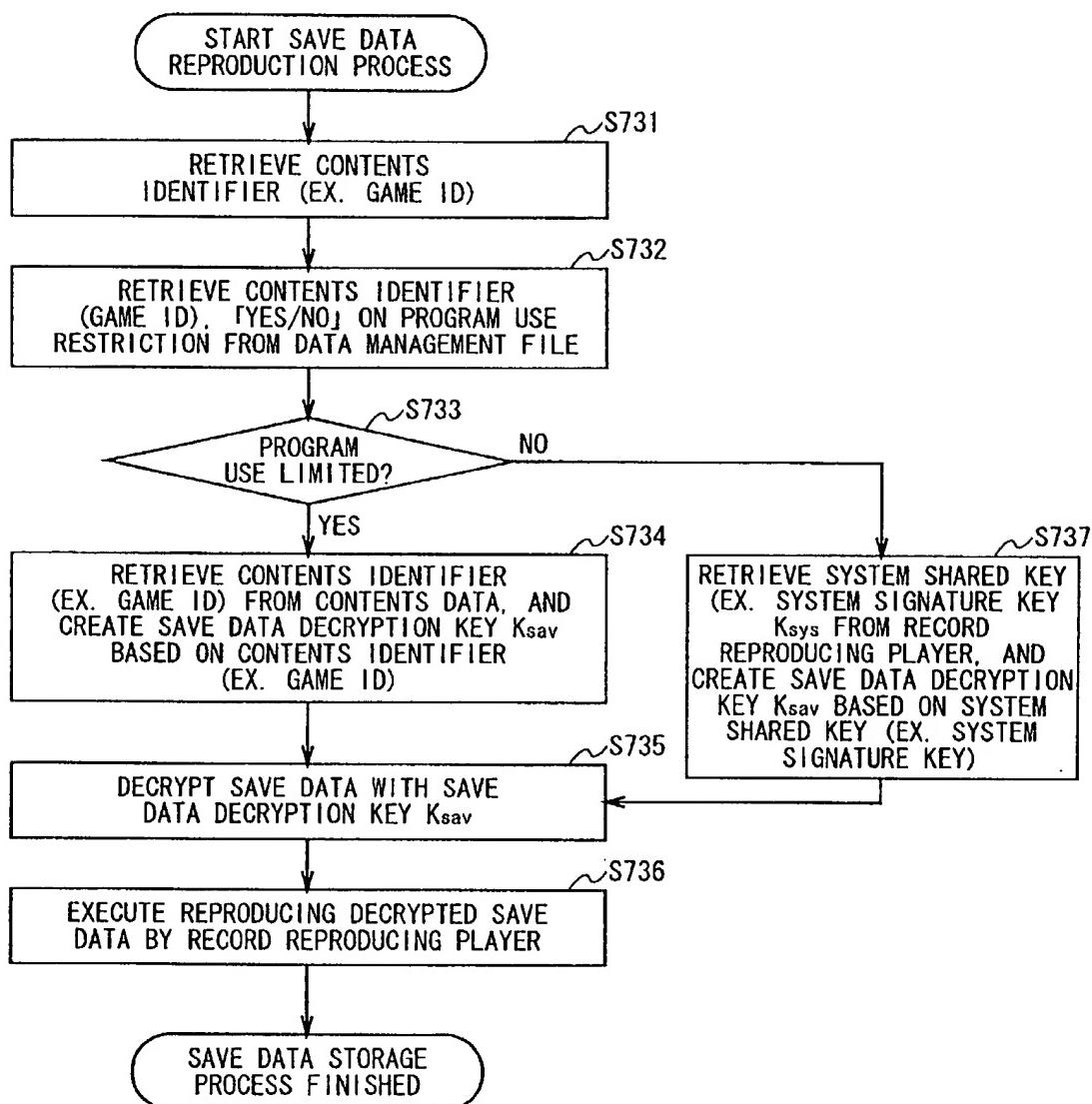


FIG. 74

(5) EXAMPLE OF SAVE DATA STORAGE PROCESS USING RECORD REPRODUCING
PLAYER INDIVIDUAL KEY, OR SYSTEM SHARED KEY

TOP SECRET//COMINT//E650

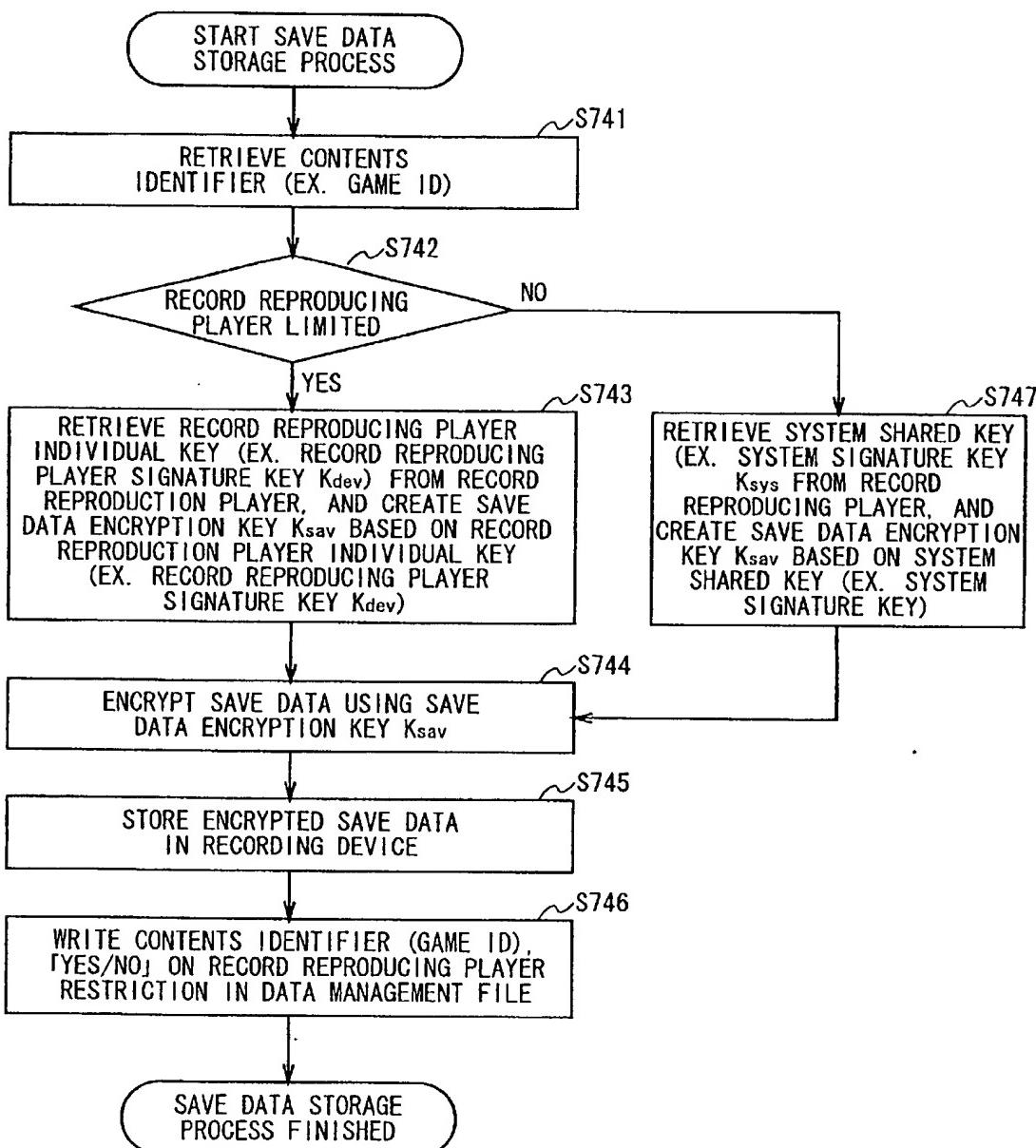


FIG. 75

TECHNISCHE UNIVERSITÄT DARMSTADT

INSTITUT FÜR INGENIEURWISSENSCHAFTEN

091937410

DATA MANAGEMENT FILE (2)

DATA NO.	CONTENTS IDENTIFIER (GAME ID)	RECORD REPRODUCING PLAYER IDENTIFIER (Id _{dev})	RECORD REPRODUCING PLAYER RESTRICTION
1	12345678...	56789012...	NO
2	ABCDEF12...	09876543...	YES
3	12245678...	58834762...	YES
:	:	:	:

FIG. 76

(6) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING RECORD REPRODUCING PLAYER INDIVIDUAL KEY, OR SYSTEM SHARED KEY

TOP SECRET//DFI//E660

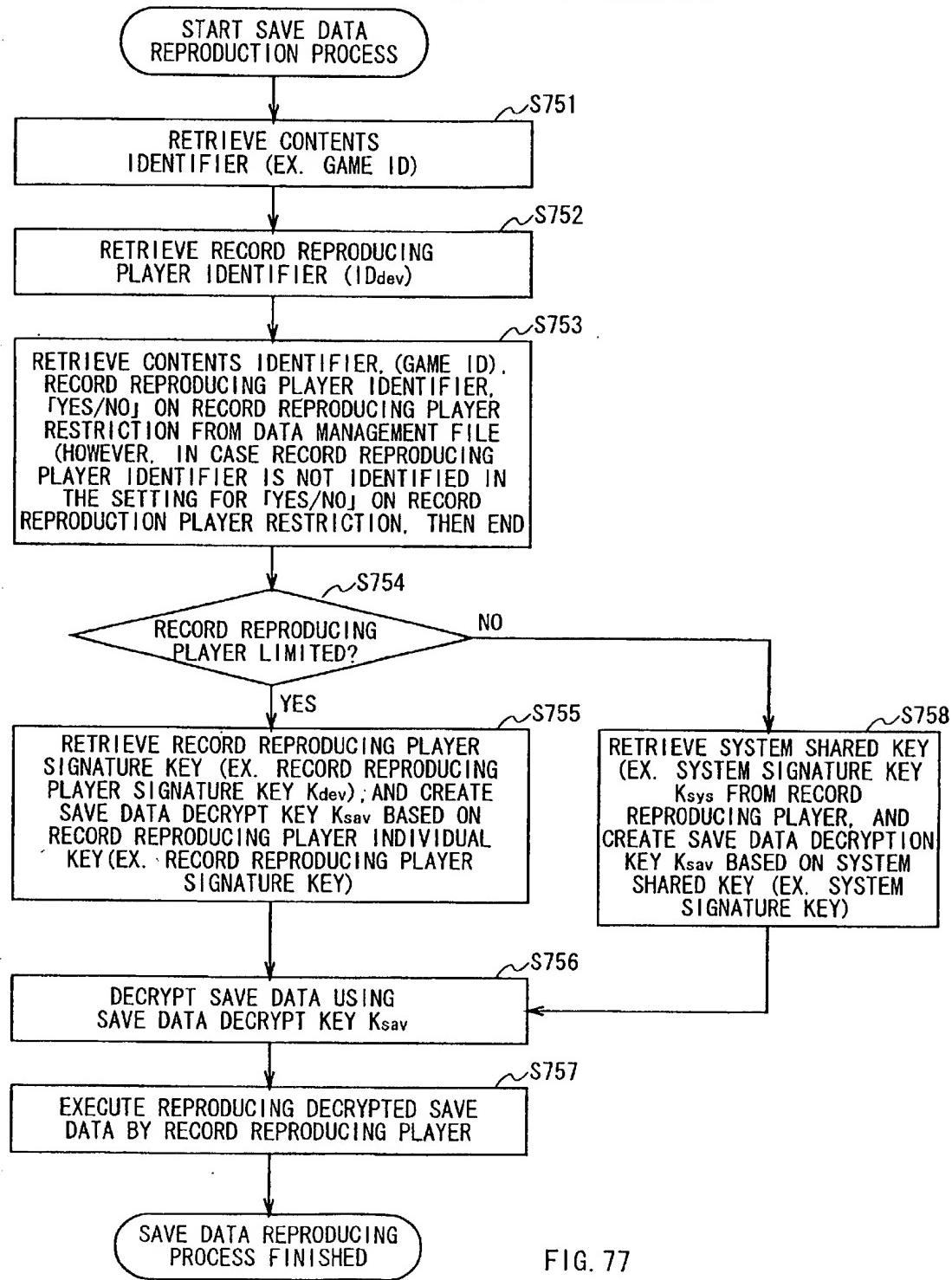


FIG. 77

(7) EXAMPLE OF SAVE DATA STORAGE PROCESS USING RECORD REPRODUCING PLAYER IDENTIFIER, OR SYSTEM SHARED KEY

TOP SECRET - OMEGASDO

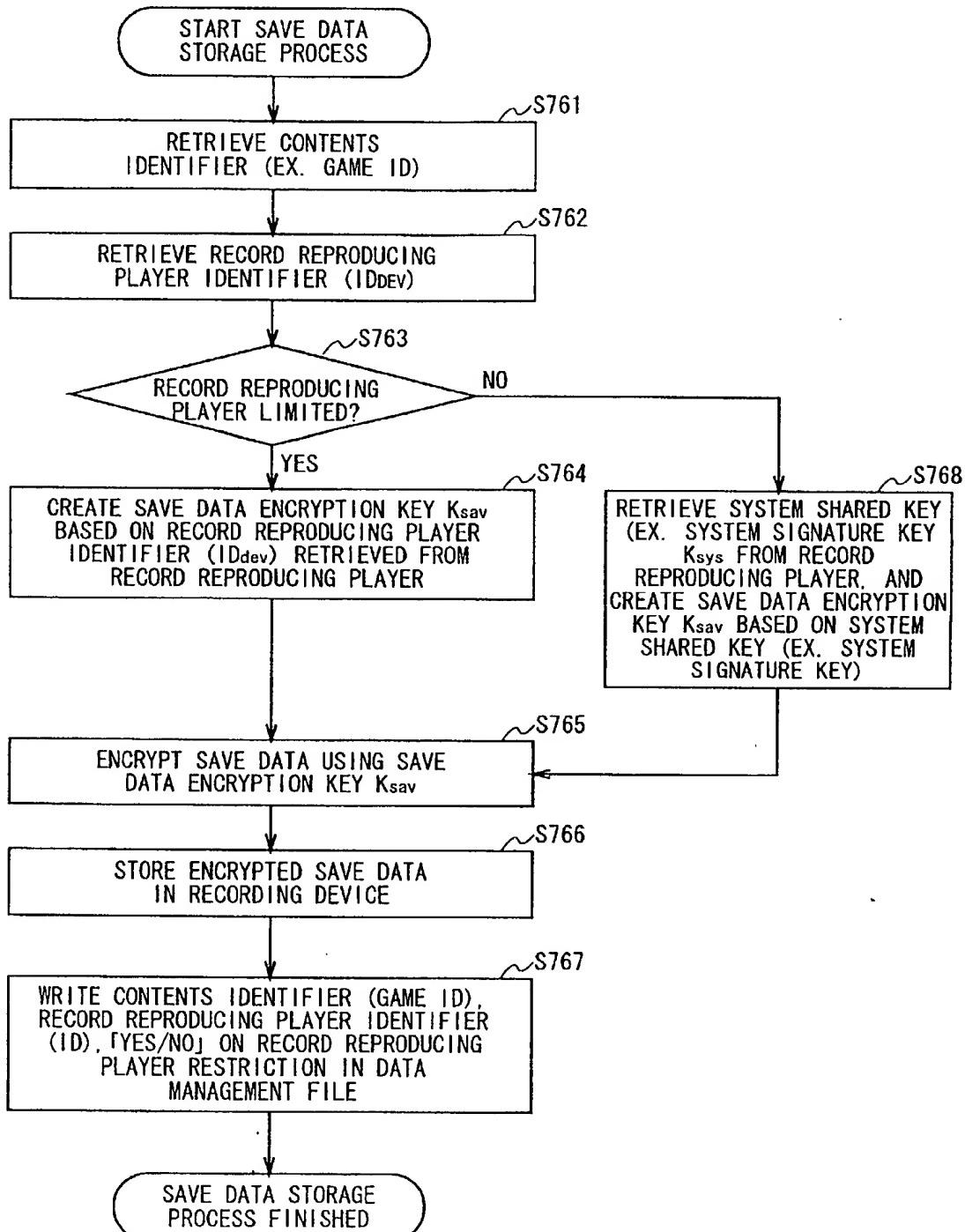


FIG. 78

(8) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING RECORD REPRODUCING PLAYER IDENTIFIER, OR SYSTEM SHARED KEY

FOURTEEN OFFICES 60

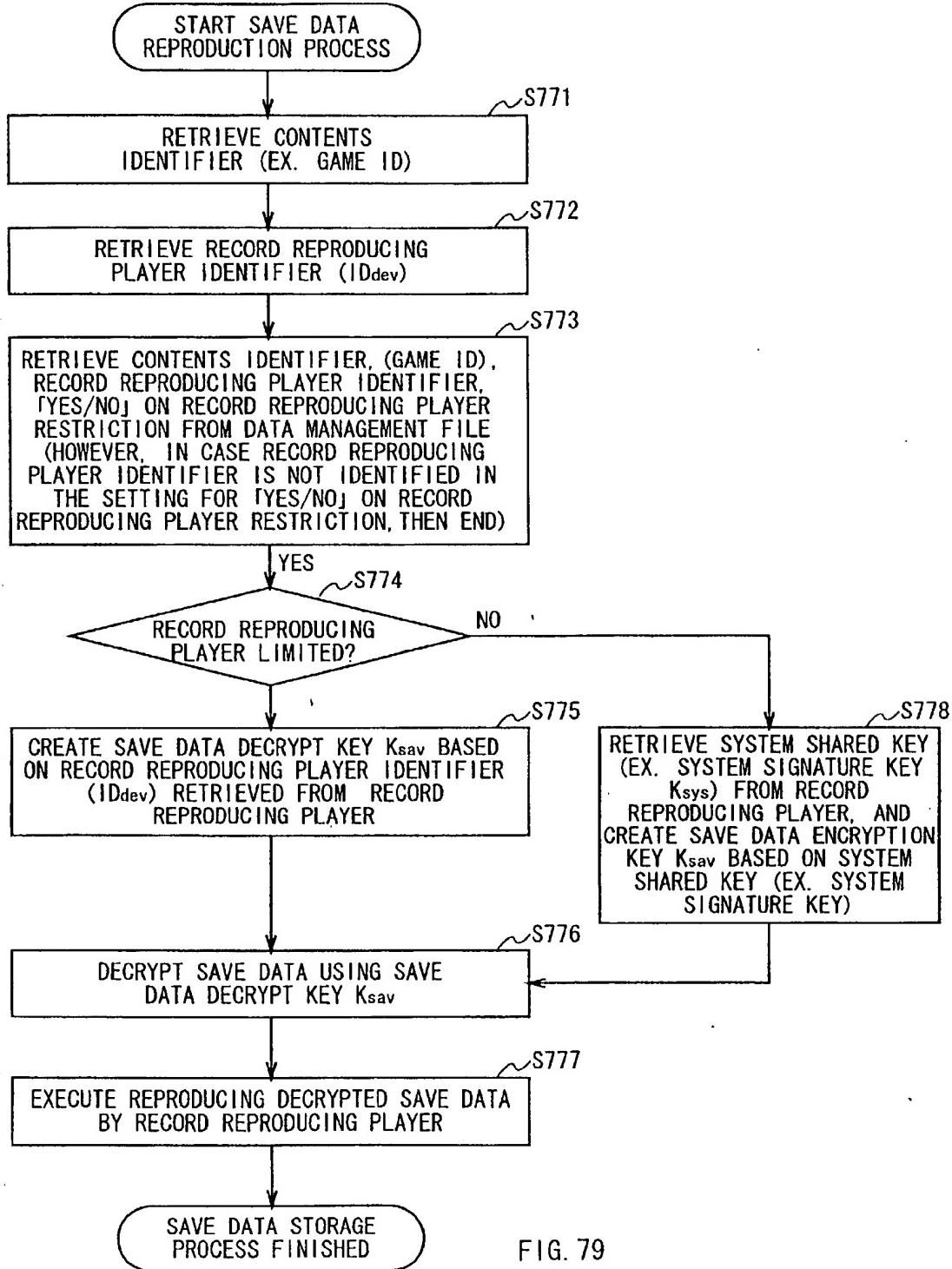
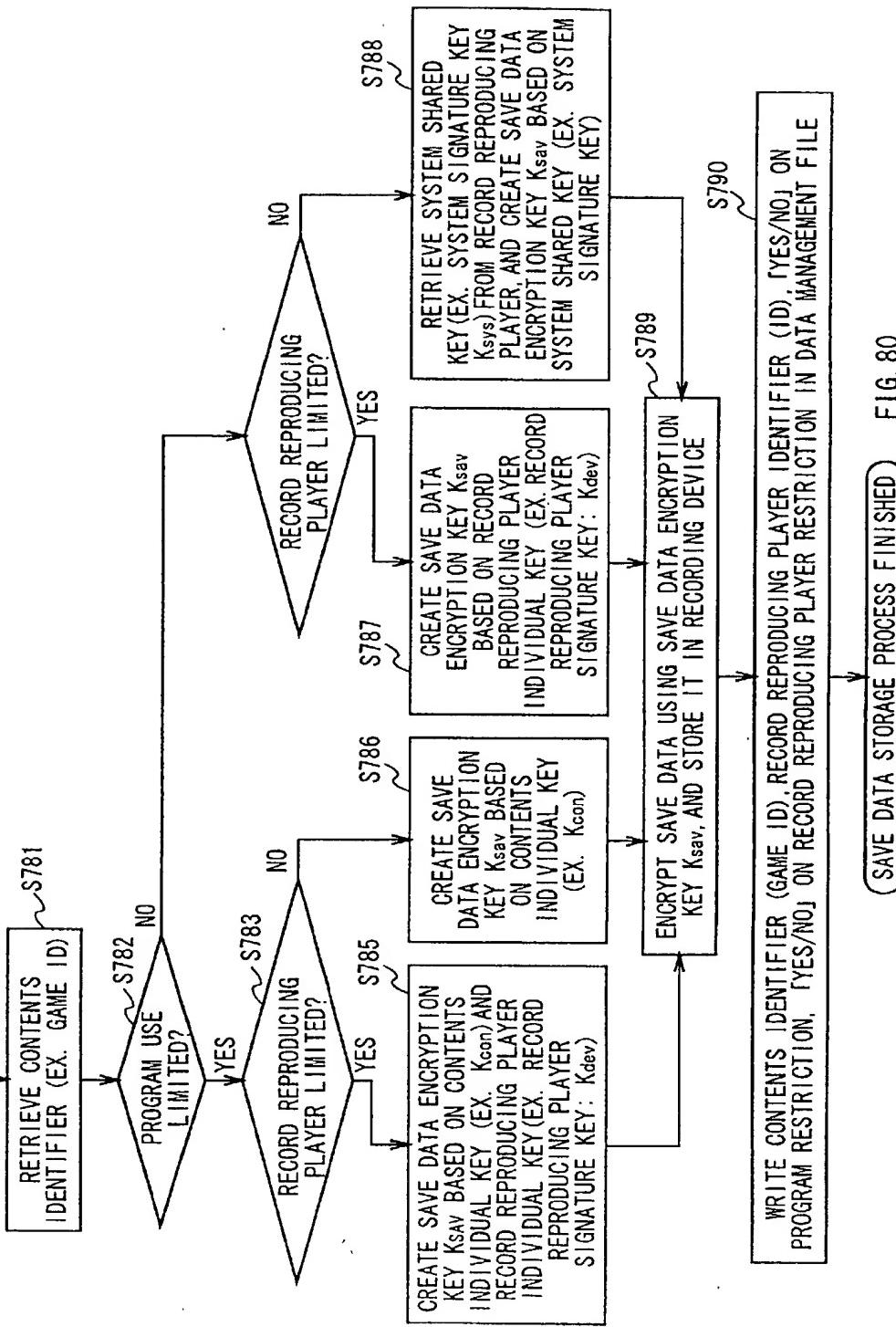


FIG. 79

09/937410

(9) EXAMPLE OF SAVE DATA STORAGE PROCESS USING CONTENTS INDIVIDUAL KEY,
RECORD REPRODUCING PLAYER INDIVIDUAL KEY, OR SYSTEM SHARED KEY

START SAVE DATA STORAGE PROCESS



09/937410

பதினாற் கிராம பகுதி

DATA MANAGEMENT FILE (3)

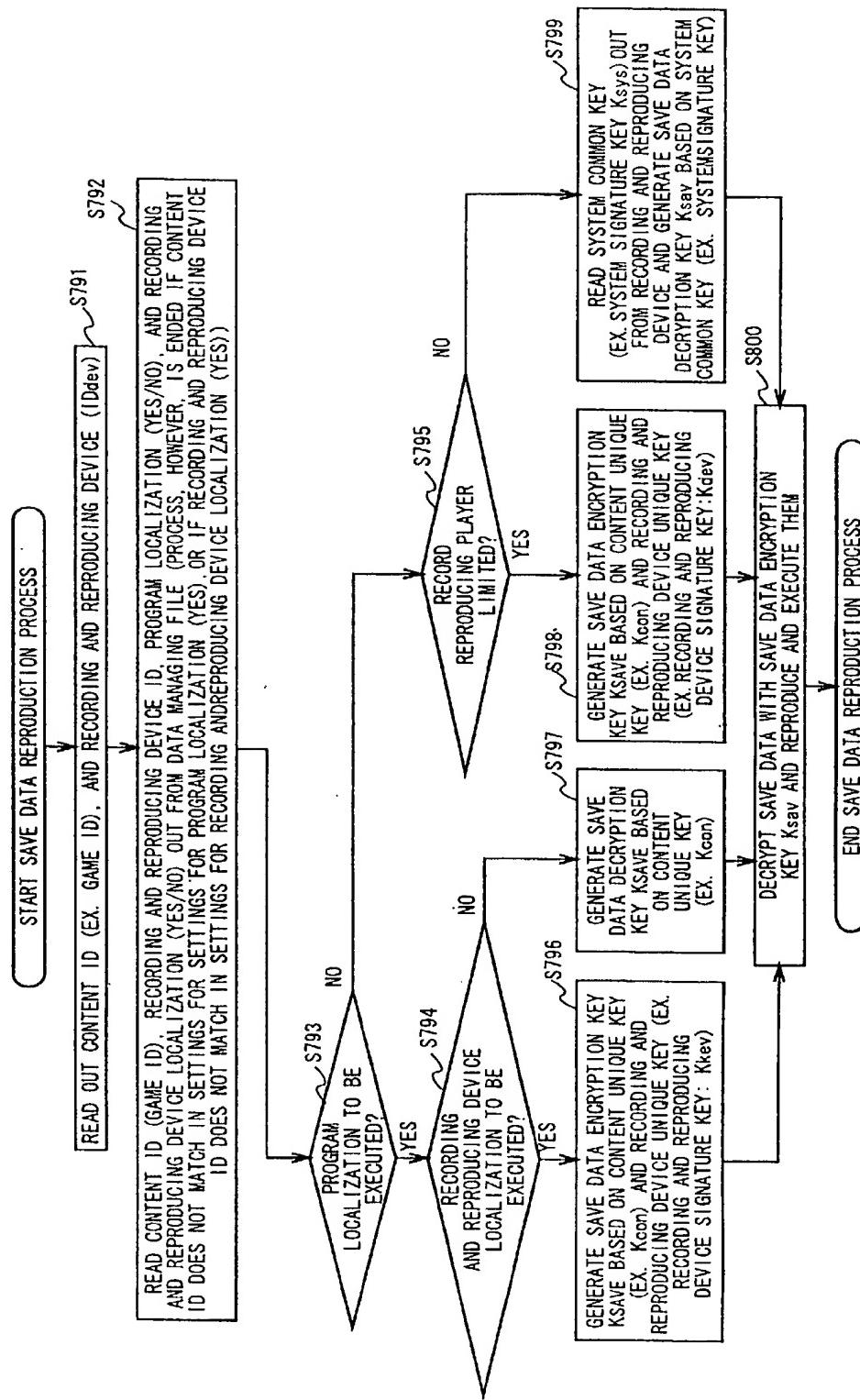
DATA NO.	CONTENTS IDENTIFIER (GAME ID)	RECORD REPRODUCING PLAYER IDENTIFIER (IDdev)	PROGRAM USE RESTRICTION	RECORD REPRODUCING PLAYER RESTRICTION
1	123455678...	56789012...	YES	NO
2	ABCDEF12...	09876543...	YES	YES
3	1122457678	58834762...	NO	YES
...

FIG. 81

80/93

09/937410

(10) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING CONTENT UNIQUE KEY,
RECORDING AND REPRODUCING DEVICE UNIQUE KEY, OR SYSTEM COMMON KEY



(11) EXAMPLE OF SAVE DATA STORAGE PROCESS USING USER PASSWORD, OR SYSTEM SHARED KEY

TOP SECRET - OFFICE OF THE CHIEF OF STAFF

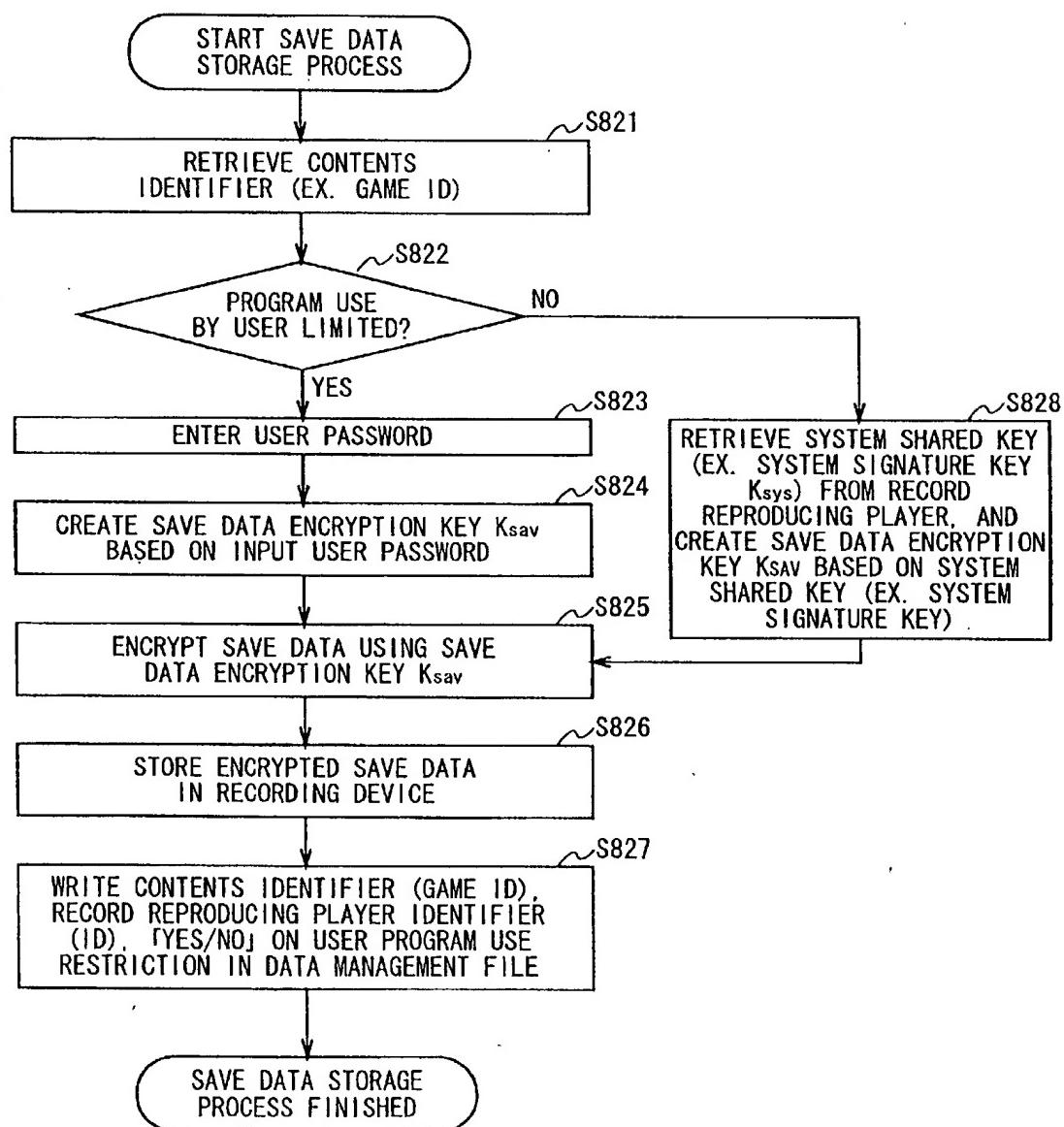


FIG. 83

09/937410

DATA MANAGEMENT FILE (4)

DATA NO.	CONTENTS IDENTIFIER (GAME ID)	RECORD REPRODUCING PLAYER IDENTIFIER (ID _{dev})	USER PROGRAM USE RESTRICTION
1	123455678...	56789012...	YES
2	ABCDEF12...	09876543...	YES
3	1122457678	58834762...	NO
•	•	•	•
•	•	•	•

FIG. 84

(12) EXAMPLE OF SAVE DATA REPRODUCTION PROCESS USING USER PASSWORD, OR SYSTEM SHARED KEY

TOP SECRET//COMINT//E60

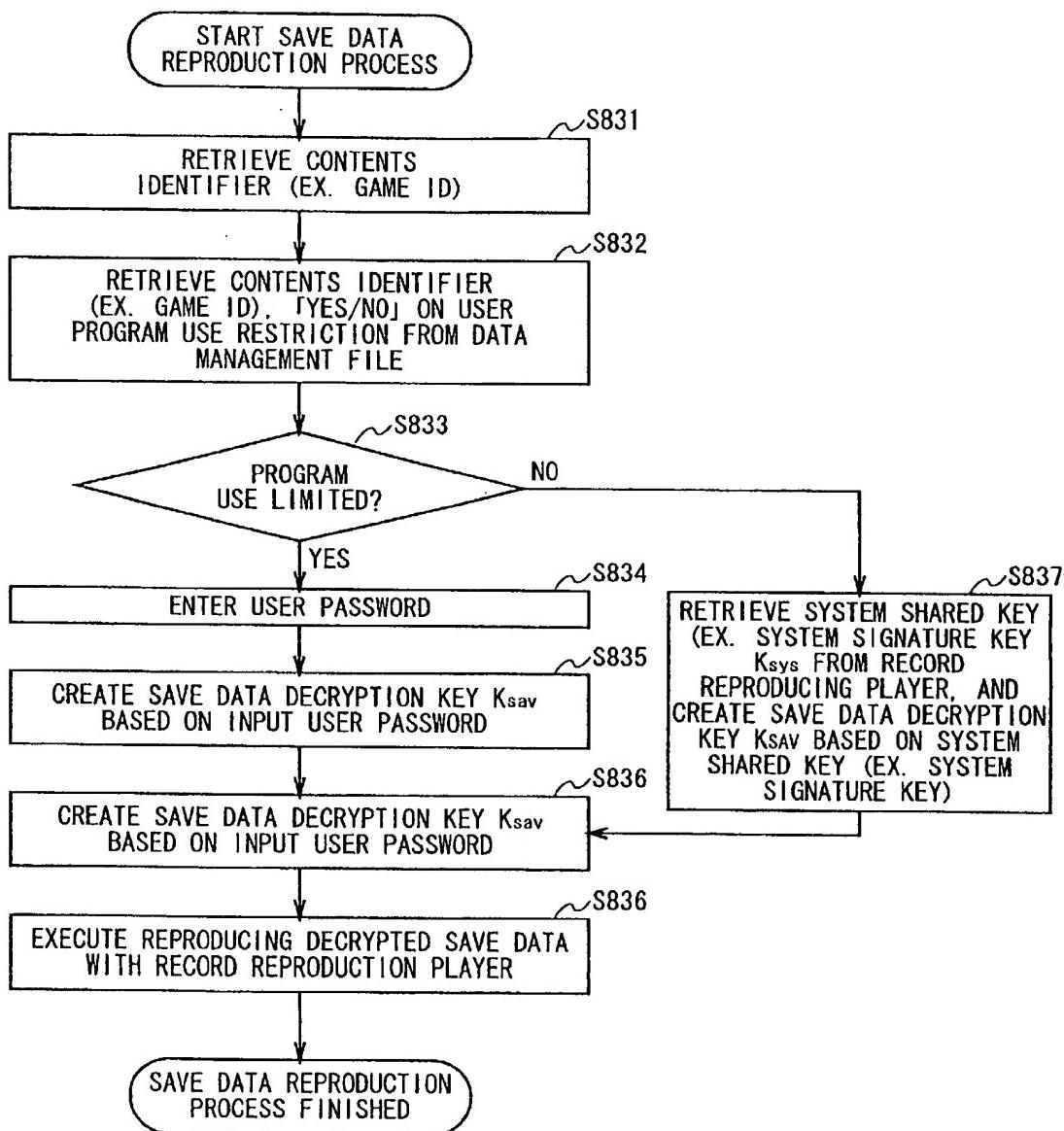


FIG. 85

09/937410

TELEFUNKEN DACHAU GMBH

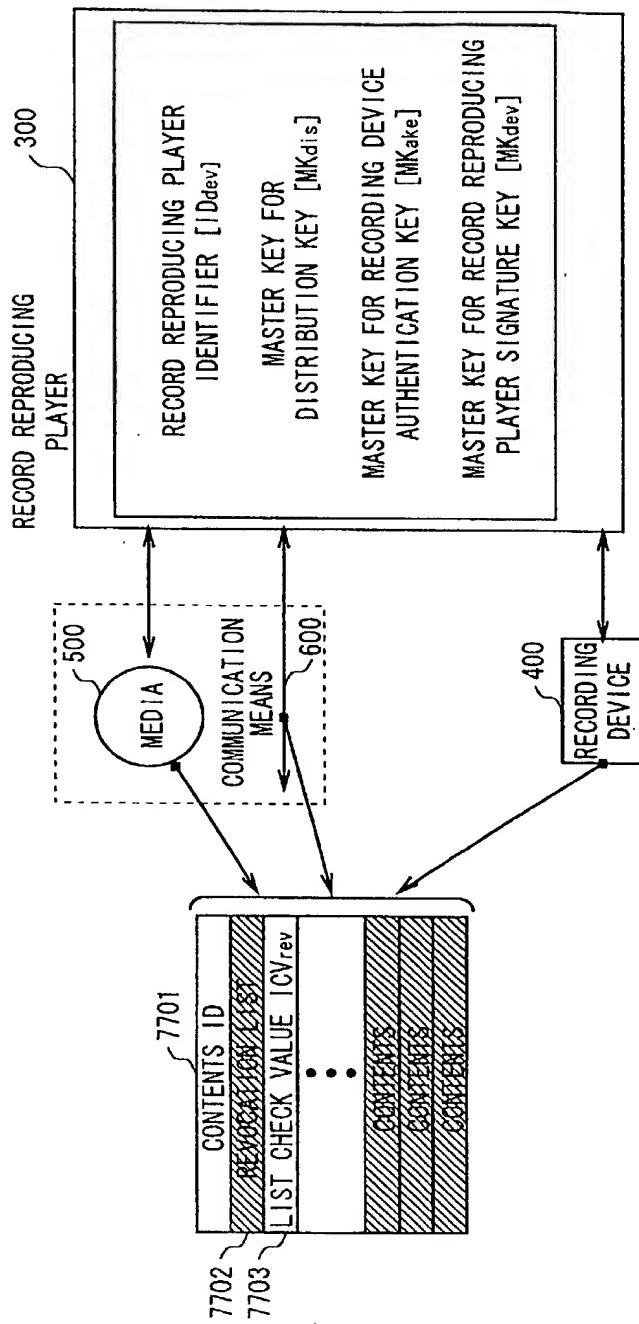


FIG. 86

TOP SECRET - OFFICE OF THE DIRECTOR

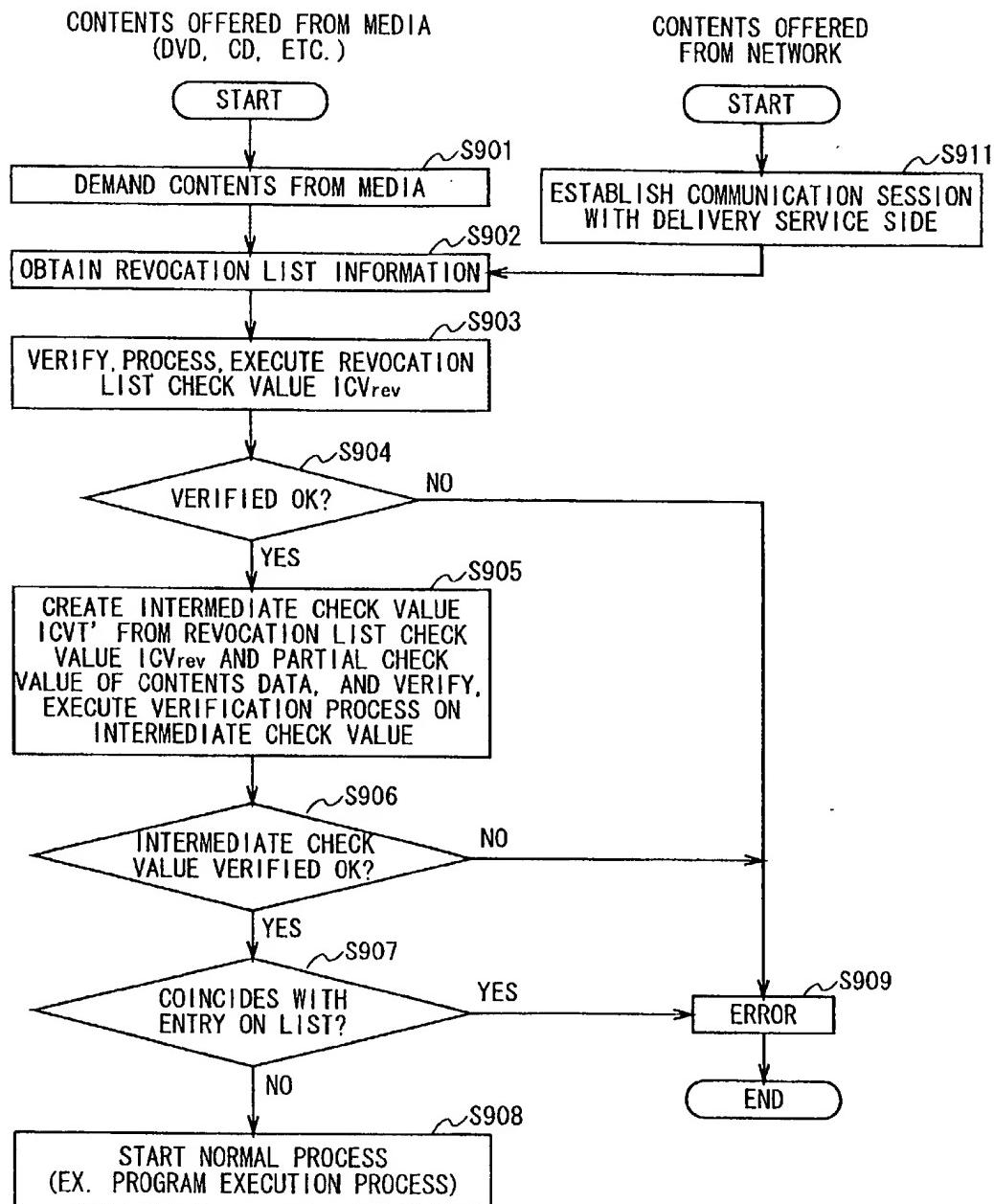


FIG. 87

TOP SECRET - OFFICIAL USE ONLY

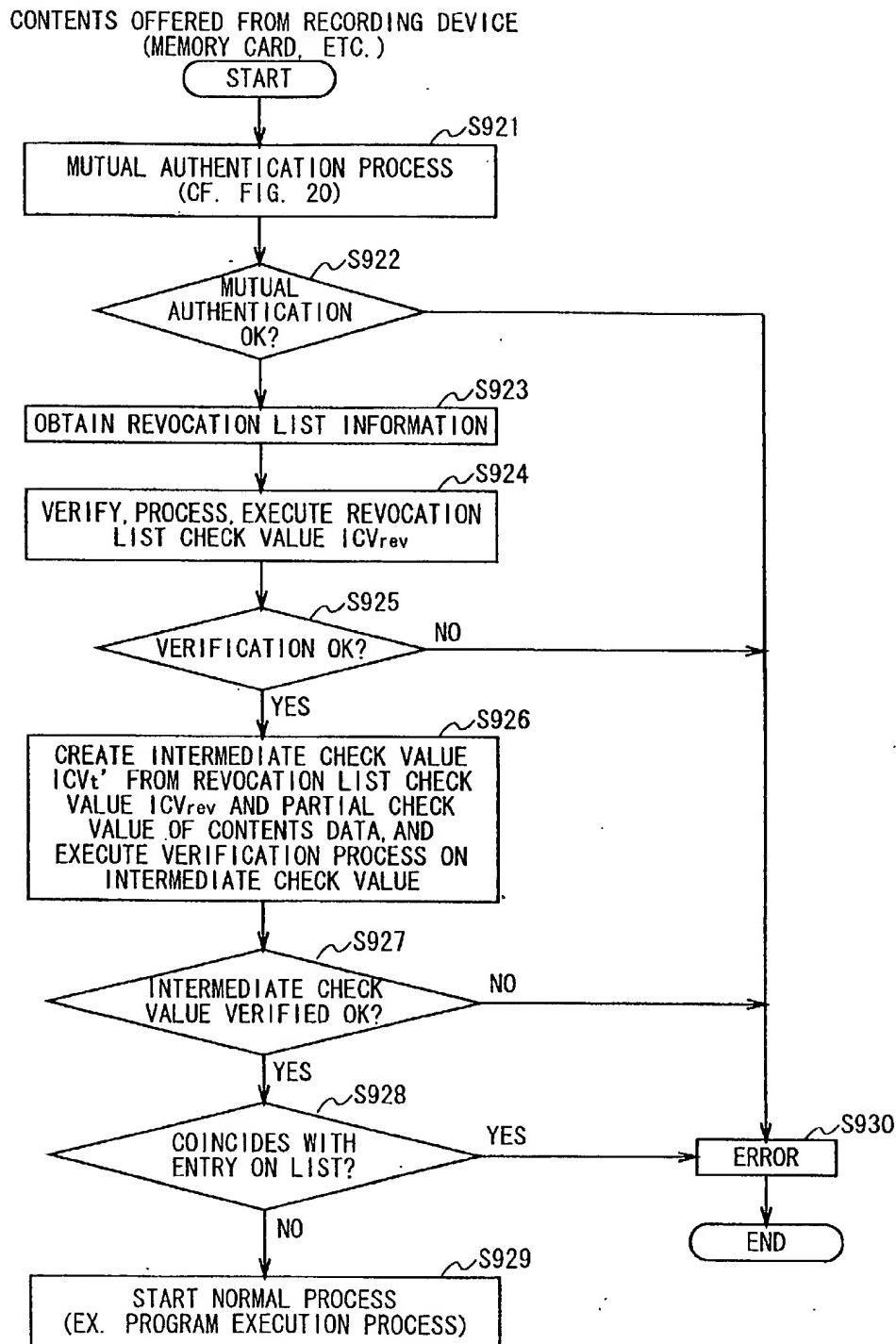


FIG. 88
87/93

09/937410

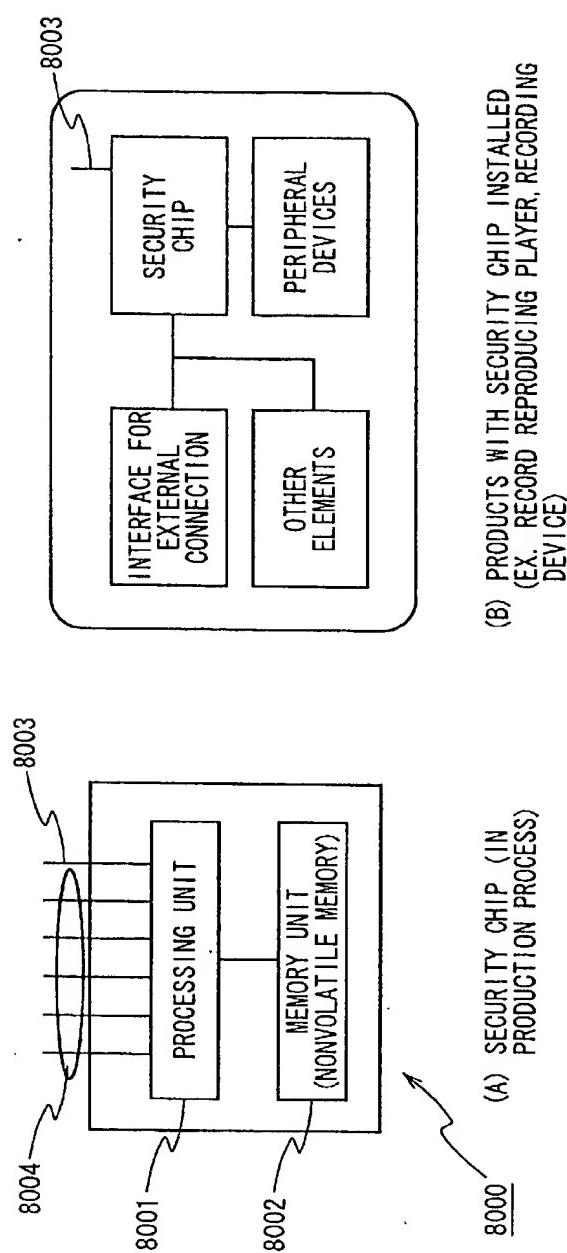


FIG. 89

TELETYPE OFFICE 6660

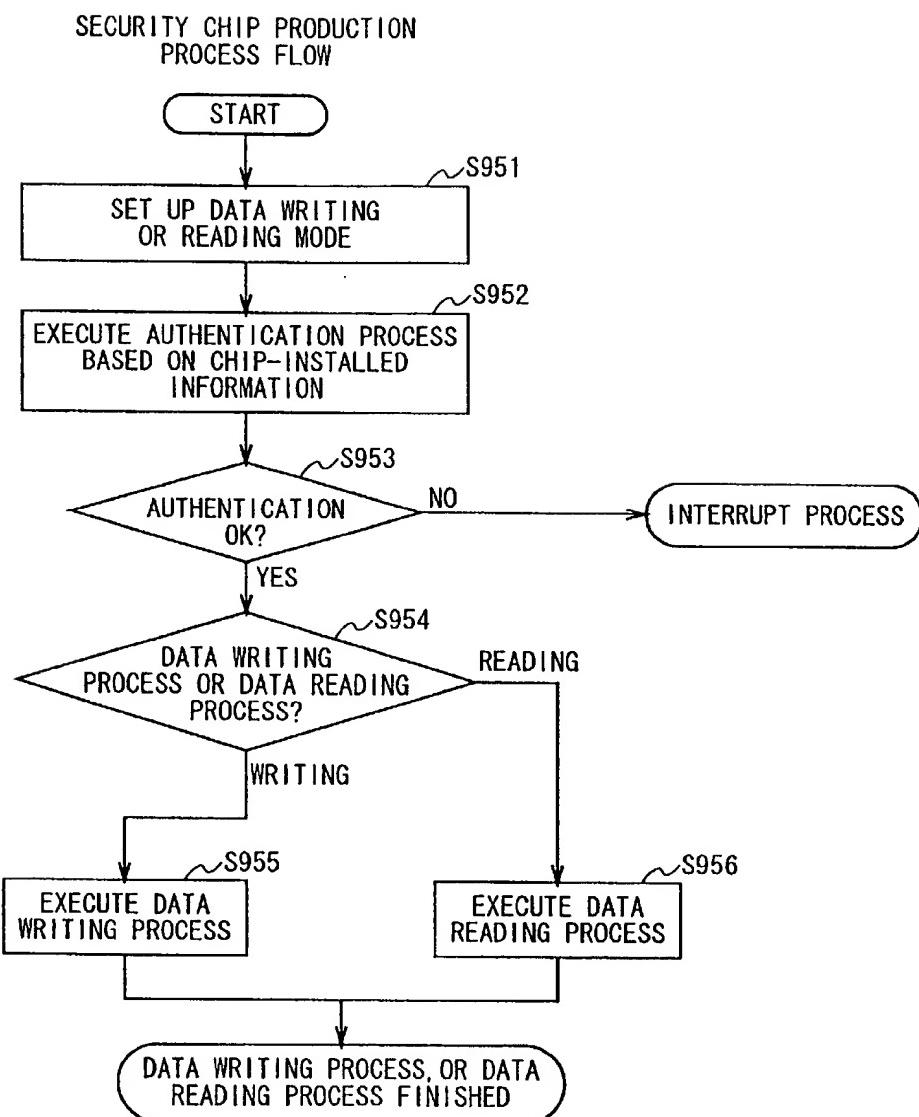


FIG. 90

09/937410

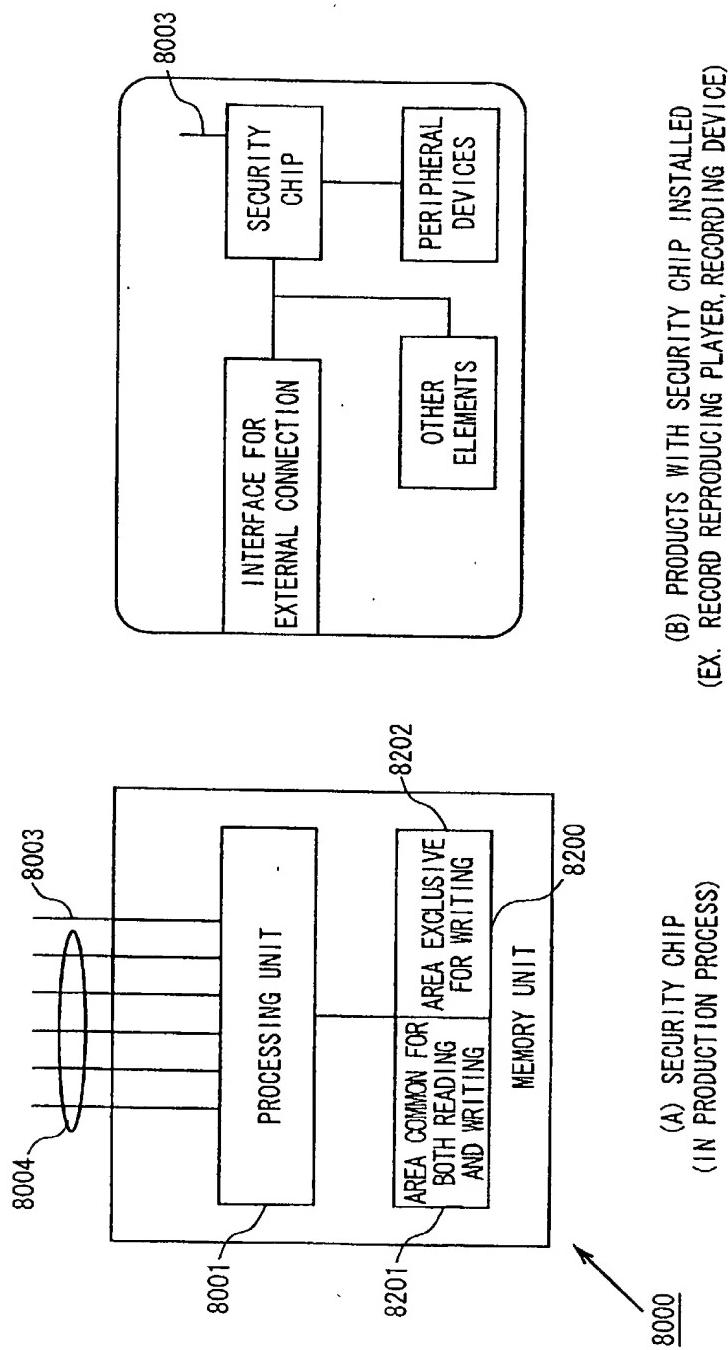


FIG. 91

FOVTEF-DT92E660

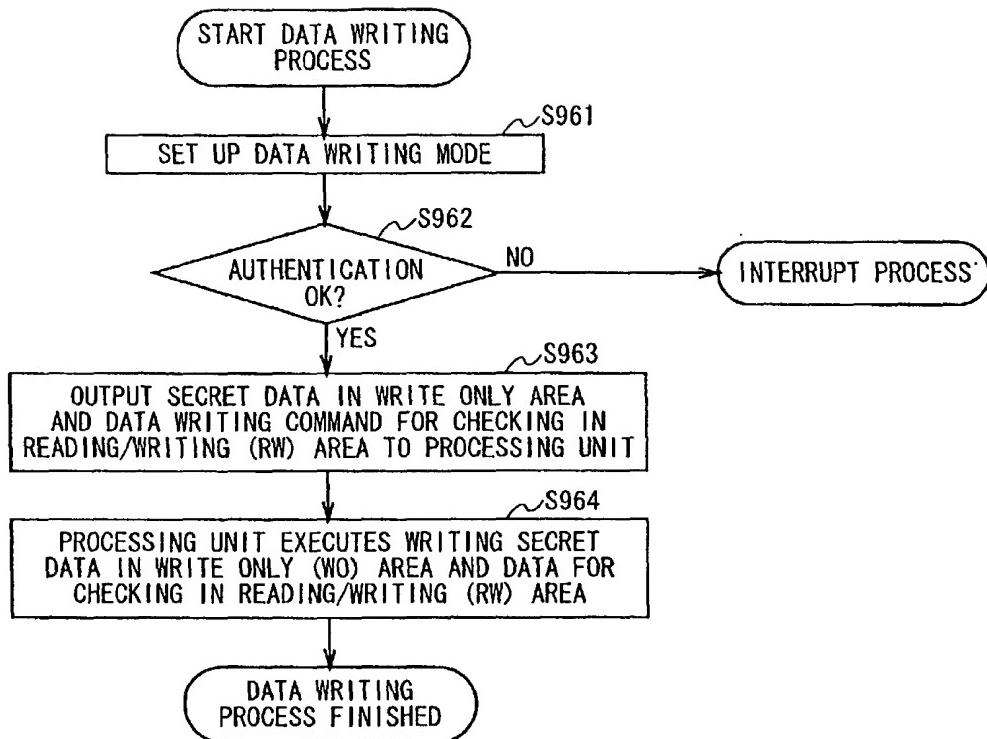


FIG. 92

09/937410

TOP SECRET - DTIC 2660

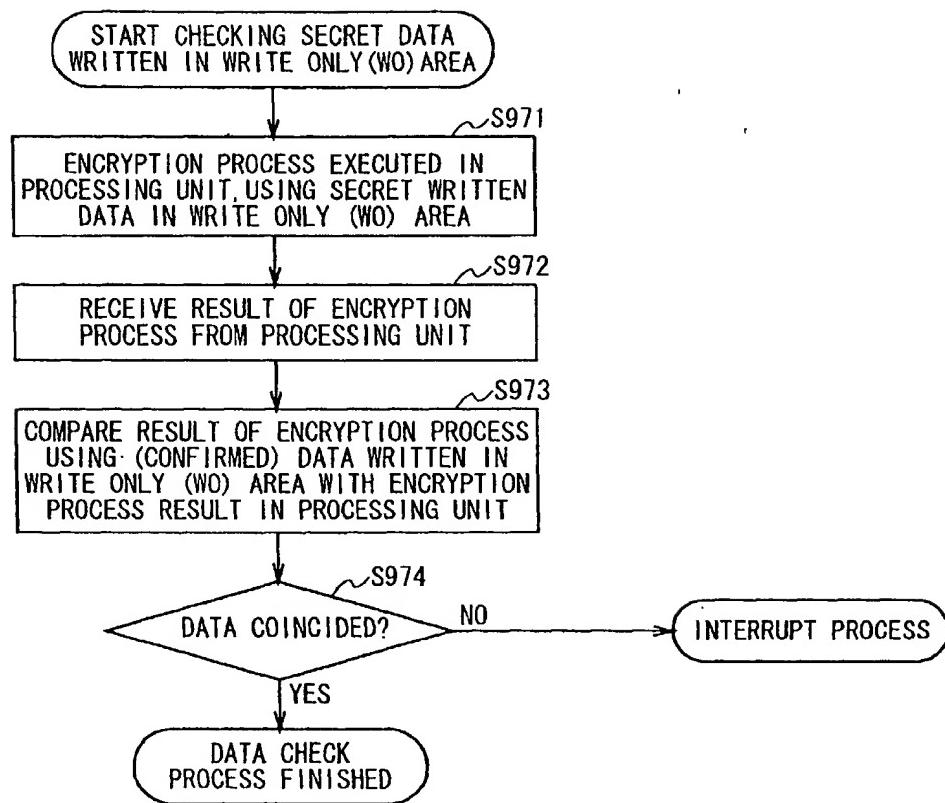


FIG. 93

09/937410

Explanation of Reference Numerals

106 -- main CPU, 107 -- RAM, 108 -- ROM, 109 -- AV processing unit, 110 -- input processing unit, 111 -- PIO, 112 -- SIO, 300 -- record reproduction player, 301 -- control unit, 302 -- encryption processing unit, 303 -- recording device controller, 304 -- read unit, 305 -- communication unit, 306 -- control unit, 307 -- internal memory, 308 -- encryption/decryption unit, 400 -- recording device, 401 -- encryption processing unit, 402 -- external memory, 403 -- control unit, 404 -- communication unit, 405 -- internal memory, 406 -- encryption/decryption unit, 407 -- external memory control unit, 500 -- media, 600 -- communication means, 2101, 2102, 2103 -- record reproduction player, 2104, 2105, 2106 -- recording device, 2901 -- command numbers management unit, 2902 -- command register, 2903, 2904 -- authentication flag, 3001 -- speaker, 3002 -- monitor, 3090 -- memory, 3091 -- contents analyzing unit, 3092 -- data memory unit, 3093 -- program memory unit, 3094 -- compression/decompression processing unit, 7701 -- contents data, 7702 -- revocation list, 7703 -- list check value, 8000 -- security chip, 8001 -- processing unit, 8002 -- memory unit, 8003 -- mode signal line, 8004 -- command signal line, 8201 -- read/write area, 8201 -- write only area